



**Assuring Safety through Operational Approval:
Challenges in Assessing and Approving the
Safety of Systems-Level Changes in Air Transportation**

Roland E. Weibel and R. John Hansman

This report is based on the Doctoral Dissertation of Roland E. Weibel submitted to the Department of Aeronautics and Astronautics in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the Massachusetts Institute of Technology.

*The work presented in this report was also conducted
in collaboration with the members of the Doctoral Committee:*

*Prof. R. John Hansman (Chair)
Prof. Annalisa Weigel
Dr. Jim Kuchar*

Report No. ICAT-2009-04
September 2009

MIT International Center for Air Transportation (ICAT)
Department of Aeronautics & Astronautics
Massachusetts Institute of Technology
Cambridge, MA 02139 USA

(this page intentionally left blank)

Assuring Safety through Operational Approval: Challenges in Assessing and Approving the Safety of Systems-Level Changes in Air Transportation

by

Roland E. Weibel and R. John Hansman

Abstract

To improve capacity and efficiency of the air transportation system, a number of new systems-level changes have been proposed. Key aspects of the proposed changes are combined functionality across technology and procedures and large physical scale of deployment. The objective of this work is to examine the current safety assessment processes for systems-level changes and to develop an understanding of key challenges and implications for the assessment and approval of future systems-level changes.

From an investigation of current U.S. and international safety regulatory policies and processes, a general model was created describing key processes supporting operational approval. Within this model, a framework defined as an influence matrix was developed to analyze key decisions regarding the required scope of analysis in safety assessment. The influence matrix represents the expected change in levels of risk due to changes in behavior of elements of a system. It is used to evaluate the appropriate scope of analysis in safety assessment. Three approaches to performing safety assessment of systems-level changes were analyzed using the framework: the risk matrix approach, target level of safety approach, and performance-based approach. Case studies were performed using eight implemented and pending systems-level changes.

In this work, challenges expected in safety assessment of future systems-level changes were identified. Challenges include the large scope of proposed changes, which drives a need for a broad and deep scope of analysis, including the multiple hazards and conditions and complex interactions between components of a change and the external system. In addition, it can be expected that high safety expectations will increase the required accuracy of models and underlying data used in safety assessment. Fundamentally new operational concepts are also expected to expand the required scope of safety assessment, and a need to interface with legacy systems will limit achievable operations. The large scope of analysis expected for future changes will require new methods to manage scope of safety assessment, and insights into potential approaches are discussed.

(this page intentionally left blank)

Acknowledgements

This work was supported by the Federal Aviation Administration under grant FAA 95-G-017. The authors wish to thank the members and technical monitors for the Joint University Program for their support and feedback for the work.

In addition, the authors thank the members of the doctoral committee: Prof. Annalisa Weigel of MIT, Dr. Jim Kuchar of MIT Lincoln Laboratory, Dr. Amy Pritchett of NASA and Dr. Tom Reynolds of MIT for their insight, review, and feedback. Thanks also go to the members of the International Center for Air Transportation, particularly Philippe Bonnefoy, Alex Mozdzanowska, and Masha Ishutkina for their support and feedback.

(this page intentionally left blank)

Table of Contents

Acknowledgements	5
Table of Figures.....	11
List of Tables	13
1 Introduction: Air Transportation System Change and Safety Assessment.....	15
1.1 Current Modernization Initiatives.....	15
1.2 Increasing Air Transportation System Safety	17
1.3 Safety Assessment In Support of Operational Approval.....	19
1.4 Scoping in Safety Assessment.....	19
1.5 Research Objective.....	20
1.6 Research Approach	20
1.6.1 Investigation of Current Safety Regulatory Policies and Processes	21
1.6.2 Synthesis of Safety Assessment Decision-Making Methods	23
1.6.3 Case Studies	24
1.6.4 Identification of Challenges and Implications for Future Air Transportation System Changes	25
2 Key Concepts and Literature Review.....	27
2.1 Operational Events and Safety.....	27
2.2 Safety Assessment.....	29
2.3 Literature Review.....	30
2.3.1 The Concept of Risk, Risk Perception, and Risk Communication	30
2.3.2 Accident Causality and Safety	31
2.3.3 New Approaches to Safety Assessment in Complex, Safety-Critical Systems	32
2.3.4 Air Transportation Change Processes	33
2.3.5 Challenges in Future Air Transportation Safety	34
3 Current Safety Regulatory Processes and Policies in US Air Transportation	35
3.1 Air Transportation System Components	36
3.2 Safety Assessment and Operational Approval of Distributed Capabilities	38
3.3 Safety Assessment.....	42
3.4 Safety Approval Processes by Air Transportation System Component	46
3.4.1 Aircraft and Airborne Equipment Certification	47
3.4.2 Certification of Airmen and Credentialing of Air Traffic Controllers.....	48
3.4.3 Operator Certificates and Operational Approval	50
3.4.4 Airspace Procedure Design & Approval.....	51
3.4.5 Separation Standards & Surveillance System Performance	52
3.4.6 Ground-Based Equipment and Programs.....	53
3.4.7 Software and Complex Electronic Hardware.....	55
3.5 Other Safety Control Processes.....	56
3.5.1 Monitoring of Current Operations	57
3.5.2 Rulemaking	57
3.6 Summary of Safety Assessment for Systems-Level Changes	58

4	Scoping in Safety Assessment and the Influence Framework.....	59
4.1	Systems-Level Operational Approval Model.....	59
4.2	Elements of a Proposed Change.....	61
4.3	The Influence of System Elements on Safety	64
4.3.1	Abstractions Used in Safety Assessment.....	64
4.3.2	Scoping in Safety Assessment	68
4.3.3	Changes in Safety Behavior due to Changes of Elements and Influence	69
4.4	Application of the Influence Matrix to Scope Decisions	73
4.4.1	Creation of Influence Matrix for a Proposed Change	73
4.4.2	Influence Matrix and Scope of Analysis.....	75
4.4.3	Elimination of Risks from Scope	77
4.4.4	Unknown Risks and Scope	80
4.5	Detailed Assessment and Modeling/ Mitigation	81
4.6	Operational Approval	82
5	Analysis of Safety Assessment Approaches Using the Influence Framework	85
5.1	Risk Matrix Approach	85
5.1.1	Hazard/Risk Identification	87
5.1.2	Scoping	88
5.1.3	Detailed Assessment and Modeling/ Mitigation.....	91
5.2	Target Level of Safety Approach	94
5.2.1	Hazard/Risk Identification	95
5.2.2	Scoping	98
5.2.3	Detailed Assessment and Modeling/ Mitigation.....	99
5.3	Performance-Based Approach	100
5.3.1	Hazard/Risk Identification	100
5.3.2	Scoping	100
5.3.3	Detailed Modeling and Assessment.....	101
6	Application of Influence framework to Safety Assessment of European Reduced Vertical Separation Minima.....	103
6.1	Overview and System Description of RVSM.....	103
6.2	RVSM Safety Assessment Approach.....	105
6.3	Application of the Influence Framework to the RVSM FHA	107
6.3.1	Methodology Applied to Create the RVSM Influence Matrix	107
6.3.2	Scoping in the RVSM Influence Matrix	110
6.3.3	Subsequent Review of FHA Hazards	113
6.4	Summary	116

7 Challenges in Safety Assessment Identified from Case Studies and Implications for Safety Assessment of Future Systems-Level Changes.....	117
7.1 Increasing Scope of Analysis Required	118
7.1.1 Challenges in Managing Complexity of Increased Scope	119
7.1.2 Use of the Influence Matrix to Structure Scope Decisions	120
7.2 Increasing Demands on the Quality of Safety Assessment	121
7.2.1 Increasing Safety Expectations	121
7.2.2 Increasing Accuracy Expected in Safety Assessment.....	122
7.2.3 Increasing Scope Required to Accurately Represent Behavior	122
7.2.4 Use of Operational Monitoring as a Mitigation	125
7.3 Assessment Challenges from Fundamentally New Types of Operations	125
7.4 Limitations in Achievable Performance due to Interaction with Legacy Systems.....	127
7.4.1 Performance Limitations of Legacy Systems	127
7.4.2 High Performance Requirements Set by Lower Performance System Elements	128
7.5 Balancing Required Performance In Long Time Scales of Change	128
7.5.1 Future vs. Current Demands for Functionality	128
7.5.2 Requirements Stability.....	130
7.6 Summary	130
8 Conclusions and Recommendations for Future Work	131
9 Bibliography.....	135
 Appendix A: Acronyms & Abbreviations.....	 145
Appendix B: Documentation of Current Safety Regulatory Processes Reviewed.....	147
Appendix C: Interviews Conducted.....	149
Appendix D: Case Studies.....	151
D.1 Initial Instrument Landing Systems (ILS).....	152
D.2 North Atlantic Organized Track System (NAT OTS)	154
D.3 Traffic Alert and Collision Avoidance System (TCAS)	160
D.4 Precision Runway Monitor (PRM)	171
D.5 Reduced Vertical Separation Minima (RVSM) in Europe (EUR).....	175
D.6 Overview of Automatic Dependent Surveillance, Broadcast (ADS-B) Cases	178
D.7 Automatic Dependent Surveillance Broadcast (ADS-B) Alaska Capstone Program	180
D.8 U.S. Deployment of Automatic Dependent Surveillance Broadcast (ADS-B)	184
D.9 Unmanned Aircraft Systems (UAS).....	189

Table of Figures

Figure 1-1: NextGen Enterprise Architecture Operational View	16
Figure 1-2: Historical Trends in Accident Rates for Civil Aviation.....	17
Figure 1-3: World Wide Commercial Jet Fleet Fatal Accidents.....	18
Figure 1-4: FAA Aviation Safety Organization Goals for Accident Rate Reductions.....	19
Figure 3-1: Air Transportation System Components Requiring Safety Approval	37
Figure 3-2: Processes Supporting Safety Operational Approval of a Systems-Level Change	40
Figure 3-3: Risk Matrix Classification of Risk	44
Figure 4-1: Safety Assessment Processes Supporting Operational Approval of a Proposed Change.....	60
Figure 4-2: System Elements.....	62
Figure 4-3: Elements of a Proposed System and Enabled Applications.....	63
Figure 4-4: State Transition Representation of Safety Behavior	65
Figure 4-5: A Hazard as an Intermediate State	66
Figure 4-6: Hybrid Bow-Tie Framework of Hazard Analysis.....	67
Figure 4-7: System Behavior with Multiple Hazards and Risk Events	68
Figure 4-8: Dimensions of Scope: Elements, Hazards, and Risks.....	69
Figure 4-9: Influence on Safety Behavior of a Proposed Change in the Bow Tie Model	70
Figure 4-10: Influence Defined.....	71
Figure 4-11: Influence Matrix.....	72
Figure 4-12: Notional Influence of System Elements on a Single Risk	73
Figure 4-13: Notional Influence Matrix and Level of Risk for a Proposed Change.....	75
Figure 4-14: Example of Hazard Mapping to Risks	76
Figure 4-15: Arrangement of Influence by Hazard vs. Risk.....	77
Figure 4-16: Scoping by Dominant Risk	78
Figure 4-17: Use of Similarity to Scope Hazards Assessed	80
Figure 4-18: Out of Scope Unknown Risks.....	81
Figure 4-19: Safety Assessment and Safety-Derived Requirements	82
Figure 4-20: Safety Assessment Processes Supporting Operational Approval of a Proposed Change.....	83
Figure 5-1: An Example Risk Matrix from the FAA ATO SMS	86
Figure 5-2: Hazard Identification.....	88
Figure 5-3: Reduction of Mitigation Effectiveness in Worst Credible System State.....	90
Figure 5-4: Correlation of Influence with Stressing Conditions.....	91
Figure 5-5: Single Hazard Assessment Decomposition.....	92
Figure 5-6: Evaluation of Groupings of Hazards (Clusters).....	93
Figure 5-7: Risk Budget Decomposition of Hazards.....	95
Figure 5-8: Methods for Setting Safety Targets	96

Figure 5-9: Disaggregation of Influence in Risk Budgeting.....	98
Figure 5-10: Influence in the Performance-Based Approach	101
Figure 5-11: Illustration of the Performance-Based Approach.....	101
Figure 6-1: Variation of Pressure with Altitude	104
Figure 6-2: Additional RVSM Flight Levels	104
Figure 6-3: TLS Decomposition for RVSM	106
Figure 6-4: RVSM Influence Matrix with Identified Clusters.....	108
Figure 6-5: RVSM System and Subsystem Hazards	113
Figure 6-6: Comparison of Influence Matrix Clusters to Review Report Hazards	114
Figure 7-1: Increasing Scope of Reviewed Changes	118
Figure 7-2: Target Levels of Safety from Cases Reviewed.....	121
Figure 7-3: Expansion of Scope of Analysis	123
Figure 7-4: Illustration of Consequences of Dominant Hazards	124
Figure 7-5: Current vs. Future Functionality and Levels of Requirements	129
 Figure D-1: Risk Budget for Automatic Landing Systems.....	 153
Figure D-2: Risk Budget Decomposition of NAT Collision Risk.....	155
Figure D-3: Illustration of TCAS Rate Reversal Logic Change.....	167
Figure D-4: Collision Avoidance Prevention Mitigations and Event Tree.....	170
Figure D-5: Andrews, et al. Analysis Results of Advanced Separation Concept.....	171
Figure D-6: PRM Risk Budget	172
Figure D-7: ADS-B Capstone Radar-Like Services Risk Matrix	181

List of Tables

Table 1-1: Categories of Documentation Reviewed	22
Table 1-2: Positions of Individuals Interviewed	23
Table 1-3: Case Studies Analyzed	24
Table 3-1: ATO SMS Severity Definitions	45
Table 3-2: ATO SMS Likelihood Definitions	46
Table 7-1: Summary of Case Studies Analyzed	117
Table D-1: Assessment Methods Used in Case Studies	151
Table D-2: Summary of NAT Lateral Separation Cases Reviewed	155
Table D-3: Example Hazard Assessment for Capstone ADS-B-Based Separation.....	182
Table D-4: Relationship of NIC/NAC Codes to Position Uncertainty	185
Table D-5: Definition of SIL Codes	185
Table D-3: Accuracy and Integrity Parameters Required for Selected Applications	186

(this page intentionally left blank)

1 Introduction: Air Transportation System Change and Safety Assessment

The air transportation system in developed countries such as the U.S. and Europe is reaching its capacity limits as evidenced by increasing delays. There is also a concern that the concepts of operation based on 1950s-era radar-based surveillance and voice communication will limit achievable future performance. To address these challenges, modernization initiatives propose to replace aging infrastructure and incorporate new operational capabilities through changes in technologies and procedures. Proposed changes to the United States air transportation system are being developed through the Next Generation Air Transportation System (NextGen) modernization initiative [1]. Similar modernization efforts are underway in Europe as part of the Single European Sky ATM Research (SESAR) program [2]. The proposed changes are of a systems-level nature, combining multiple components over large physical scale with significant procedural changes to achieve new operational capabilities.

A key requirement in implementing changes to the air transportation system is to assure that safety is maintained. This is achieved, in part, through the processes of safety assessment and operational approval. Motivated by the scale of proposed changes, this work seeks to develop an understanding of key processes needed for their safety assessment.

1.1 Current Modernization Initiatives

In the United States, air transportation system modernization initiatives have been proposed as part of the Next Generation Air Transportation System (NextGen). The goal of implementing NextGen capabilities is to improve the performance and efficiency of the U.S. air transportation system. The improvements envisioned in NextGen are large in physical scale; rely on distributed capabilities across multiple system components; and represent fundamentally new operational capabilities. This is illustrated by the operational view of the NextGen architecture in Figure

1-1. There are substantial stakeholders involved, significant changes to airspace operations, and a broad impact on multiple air transportation system domains.

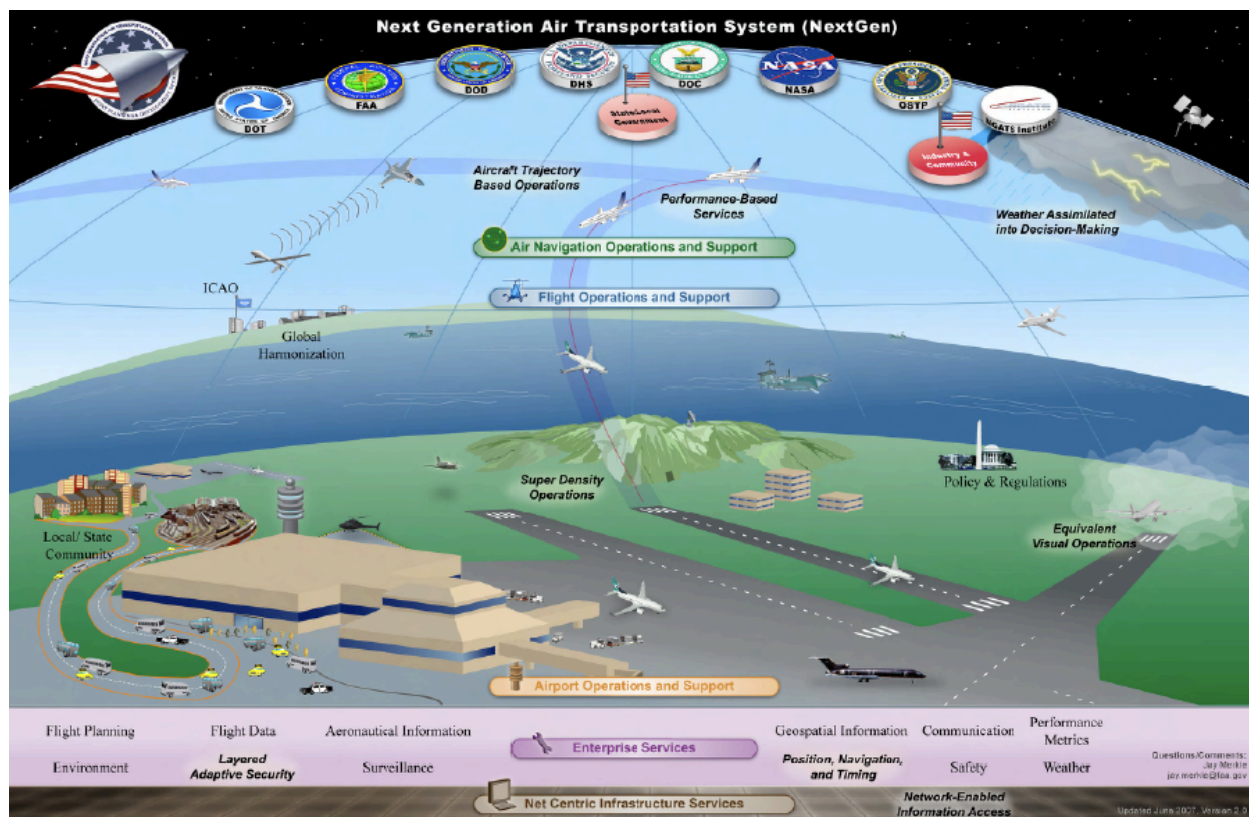


Figure 1-1: NextGen Enterprise Architecture Operational View [3]

NextGen improvements incorporate new functional capabilities into the air transportation system. An example is trajectory-based operations, which will add the dimension of time to management of air traffic. Foundational technologies, such as Automatic Dependent Surveillance Broadcast (ADS-B) and data communication are also proposed to increase air traffic control performance and efficiency.

The air traffic management system in Europe faces similar challenges to the United States. The corresponding modernization initiative, SESAR, is similar in philosophy to the NextGen vision, and contains generally similar initiatives [4].

1.2 Increasing Air Transportation System Safety

There is a general trend of increasing safety in air transportation. This trend can be seen for United States general aviation and commercial airlines in Figure 1-2. The total accident rate per hour of operation has been reduced by a factor of 10 since 1940 for general aviation, and factor of nearly 1,000 for commercial airline operations. The 5-year average accident rate for scheduled air carrier operations from 2004-2008 was 7.7 fatal accidents per 10 million hours of operation [5]. For general aviation, the rate of fatal accidents in the same time period was 1.3 per 100,000 hours of operation.

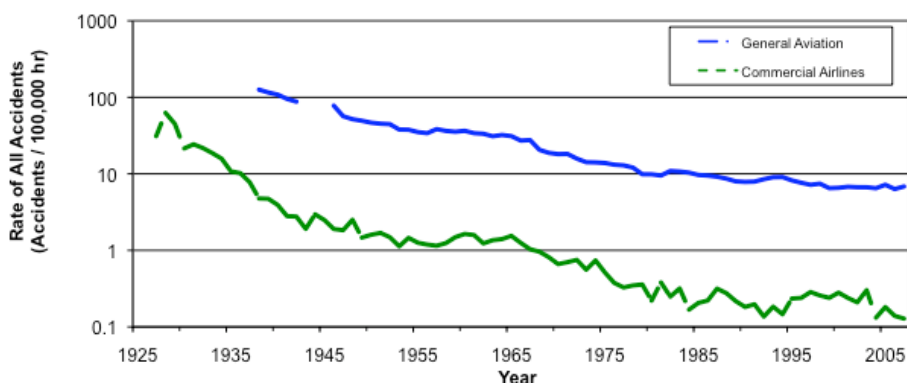


Figure 1-2: Historical Trends in Accident Rates for Civil Aviation¹

By another view, the rate of fatal accidents per million hours for the worldwide commercial jet fleet has been steadily decreasing, as shown in Figure 1-3, reported by Boeing [6]. For U.S. & Canadian operators, the rate has steadily declined from 1990-2004 as shown in the inset, but has exhibited a small increasing trend from 2004-2008. However, fatal accident rates remain at low levels, as can be seen for the broader range of data shown on the main chart.

The air transportation system in the United States and Europe is the safest form of transportation in the world. The currently high safety of the system is the result of significant advances, including implementation of specific technologies and changes to operational procedures and training over a long time scale of operation.

¹Created from general and commercial aviation accidents statistics were from the National Transportation Safety Board [17]. Historical general aviation accident statistics were obtained from the AOPA Air Safety Foundation and commercial aviation from the Bureau of Transportation Statistics.

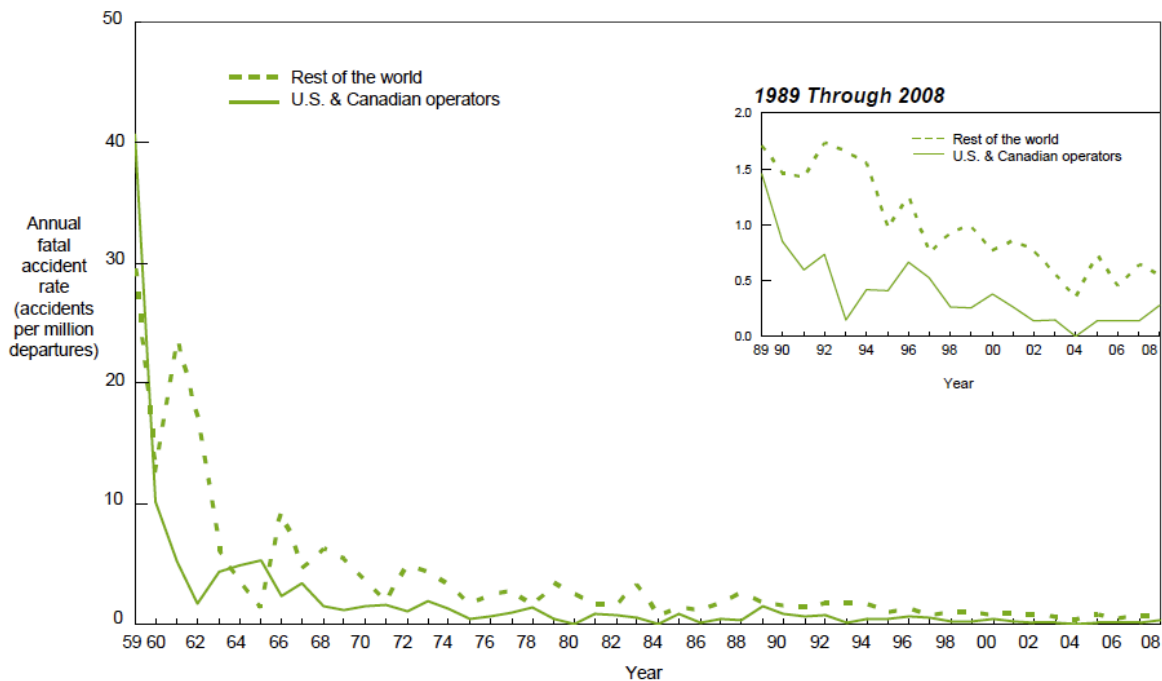


Figure 1-3: World Wide Commercial Jet Fleet Fatal Accidents [6]

It will be necessary to maintain or enhance safety in changes to the system. The currently low accident rate can therefore be expected to result in continued high demands for safety performance. Consistent with the need to enhance safety, FAA Aviation Safety Organization recognizes goals for aircraft accident rate reductions [7] shown in Figure 1-4. The figure shows baseline accident and fatality rates and planned reductions projected from the baseline year, indicated by arrows. The goals set by the FAA include a 16% reduction in the accident rate for General Aviation (GA) and non-scheduled Pt. 135 (charter) operations, and an 80% reduction in airline fatal accident rates by 2010.

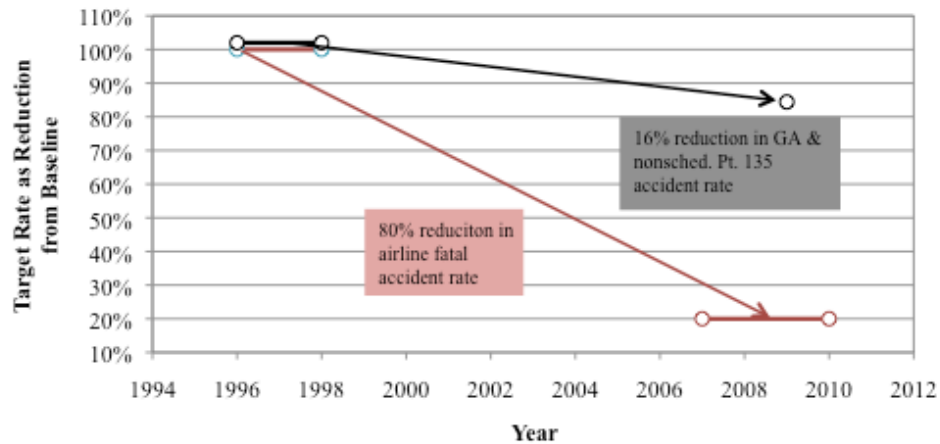


Figure 1-4: FAA Aviation Safety Organization Goals for Accident Rate Reductions

1.3 Safety Assessment In Support of Operational Approval

Several types of regulatory approval are required before overall operational approval of a proposed change. Airborne components, such as avionics, flight crews, and aircraft are certified to Federal Aviation Regulations. Certification is a guarantee to the public that these components meet minimum established performance criteria. In addition, organizations that operate aircraft, such as commercial airlines, are certified for operations. Regulators approve airspace and Air Traffic Control procedures and ground components based on internal policies, in contrast to certification to regulations. Ground equipment has historically been from external vendors and is subject to formal acquisition milestones, which include safety approval of the systems.

Civil aviation authorities typically require a safety analysis process prior to granting operational approval of proposed changes. The purpose of the analysis is to ensure that changes can be implemented at an acceptable level of safety. Various approaches can be used to conduct safety assessment, including assessment to levels of risk or derivation of performance in comparison to reference systems with similar functionality [8].

1.4 Scoping in Safety Assessment

In safety assessment of a proposed change, complex safety behavior in a real system is simplified to make analysis tractable. The scope of analysis is therefore limited, to ensure that the set of safety behavior evaluated in safety assessment is representative of the key areas of concern in the proposed change, while remaining sufficiently simple to analyze and understand.

Simplifications can be made in several areas of safety assessment. Evaluated operational conditions can be limited, such that assessment considers only the worst possible system states. Human behavior can be simplified, focusing on probabilistic estimation of the performance of humans in committing errors, or in responding to dangerous conditions. Functional interactions and system models may also be simplified depending upon the conditions that are evaluated.

Scoping decisions made in the safety assessment of a change influence the quality and validity of the safety assessment. Inappropriate constraints in scope can lead to unexamined safety behavior that can reduce the safety when the system is implemented. An inappropriately large scope can also lead to overspecification. Mitigations applied can potentially be expensive to implement, and should only be required when necessary to achieve safe operation. An inappropriately large scope can result in mitigating already acceptable risks. With the increased complexity expected in future changes, it is important to understand the implications of scoping decisions made through different safety assessment processes. It is also important to understand the potential limitations of current approaches to safety assessment and approval that may present challenges for approval of future systems.

1.5 Research Objective

Because of the large scale of proposed changes and high safety expectations, it is likely that safety assessment processes will be a significant challenge for future systems-level changes. Therefore, the objective of this research is to understand current approaches to safety assessment, with a key focus on corresponding methods for scoping analysis. Through this understanding, a further objective is to identify key challenges and implications for safety assessment of future changes.

1.6 Research Approach

The research objectives outlined above are achieved through a grounded theory approach [9]. This approach identifies key factors that define decisions made in the safety assessment of a proposed systems-level change. The analysis of safety assessment decisions was initially constructed from an investigation of current safety regulatory practices. It was then reinforced through case studies of past and pending changes. From this analysis, it was then possible to

identify expected challenges in safety assessment and operational approval of future systems-level changes.

The steps taken in the approach are listed below and briefly described in the following sections.

- Literature review
- Investigation of current safety regulatory policies and processes
 - Review of regulatory policy and process documentation
 - Interviews of personnel experienced in regulatory policy
 - Monitoring of several active change efforts (e.g. Unmanned Aircraft Systems and Automatic Dependent Surveillance, Broadcast)
- Synthesis of current regulatory practices into a general framework describing methods and decisions in safety assessment processes supporting operational approval
- Use of framework to conduct detailed case studies of specific air transportation system changes that required safety assessment and operational approval
- Application of the framework to identify challenges and implications for future air transportation system changes

1.6.1 Investigation of Current Safety Regulatory Policies and Processes

National civil aviation authorities (e.g. the U.S. FAA, Australia's CASA, etc.) have implemented different policies and processes for operational approval. To enable a detailed review, the investigation of current policies and processes was specifically focused on the safety regulatory practices of the U.S. Federal Aviation Administration (FAA).

Where appropriate, the review was extended to International Civil Aviation Organization (ICAO) policies and practices, as these serve as guidance for national regulatory policies. In some cases, safety assessment or standard development is performed by external consensus groups (e.g. RTCA, Inc) or international bodies (e.g. ICAO) with the involvement of FAA and industry personnel. These practices were also within the scope of the review. In addition, European safety regulatory policies and processes in for assessing Air Traffic Management (ATM) systems were reviewed from Eurocontrol, the European Air Navigation Service Provider (ANSP).

As shown in Table 1-1, there were seven types of documentation reviewed. *FAA regulations* for aircraft airworthiness and certification processes define required performance of systems, and

required process steps. *Advisory materials* provide acceptable means of compliance with regulations. *Orders* and *notices* described policies and practices for safety regulation. In addition to FAA regulations, *international standards and processes* also govern certification practices for some components of the air transportation system. *Handbooks and manuals* offer explanatory guidance on conducting safety assessment or systems engineering processes. Finally, *consensus standards* are established by advisory bodies and were used to examine safety performance required for specific systems. Consensus standards also contain methods for conducting safety assessment processes.

Table 1-1: Categories of Documentation Reviewed

Regulations (FAA) – defined legal standards for elements of air transportation system -Aircraft Airworthiness -Certification Processes Advisory Circulars (FAA) – acceptable means of compliance with regulation Orders (FAA) – internal policy established by FAA lines of business -Organizational: define roles and responsibilities of organizations -Process: describe processes and requirements Notices (FAA) – temporary policy established by FAA lines of business	International Standards and Processes —guidance material and requirements for signatory nations (ICAO) or EU -Safety Management Systems -Requirements for ATC Changes Handbooks & Manuals (FAA) —explanatory guidance on performing safety management functions -System Safety -Safety Management System -Systems Engineering Consensus Standards (RTCA, SAE) – standards established by advisory bodies for processes and products -Safety assurance of software and hardware -System specifications
---	---

Interviews with regulatory personnel were also conducted. The interviews served several purposes. They augmented the regulatory practice review by clarifying areas of conflicting policy. Additionally, they provided insight into practices that were not documented. The interview subjects also provided information that supported regarding studies of changes that were currently in process and initially identified challenges expected in approval of future systems. The list of the titles and organization of interview subjects is shown in Table 1-2. The names of individuals are included in Appendix C. Where appropriate, supporting evidence obtained from the interviews were used and referenced in the body of the work.

During the course of this research, insight was also gained into current FAA regulatory practices and operational approval decision-making through participation in change initiatives that are currently in progress. This included participation in several Unmanned Aircraft System (UAS)

change efforts in collaboration with NASA, FAA, MITRE, and the Department of Defense (DoD). In addition, insight was gained into Automatic Dependent Surveillance, Broadcast (ADS-B) decision-making through monitoring of efforts to identify costs and benefits, and provide feedback to the Notice of Proposed Rulemaking (NPRM) through an Aviation Rulemaking Committee.

Table 1-2: Positions of Individuals Interviewed

Title & Organization	Date (s) Interviewed
Aerospace Engineer, FAA Small Airplane Directorate, Standards Office	4/17/2007
ADS-B Separation Standards Analysis Group, Johns Hopkins University	4/25/2007
Aerospace Engineer, Avionics Systems, FAA Aircraft Certification Service	5/10/2007
Manager, DoD Joint Integrated Product Team for UAS Airspace Access	7/20/2007
Flight Test Engineer, FAA Small Airplane Directorate	4/20/2007
Manager, Air Traffic Management, International Civil Aviation Organization	5/14/2007
Staff Member, MIT Lincoln Laboratory	5/11/2007 7/16/2007
Manager, Avionics Systems, FAA Aircraft Certification Service	5/10/2007
Senior Manager, Air Traffic Operations, Fedex Aviation	4/17/2007

As a result of these activities, a detailed review of current US safety regulatory policies and processes is provided in Chapter 3. This review provides a description of the assessment and approval processes for air transportation systems, and provides background for the activities performed to assess and approve of systems-level changes that are the focus of this work.

1.6.2 Synthesis of Safety Assessment Decision-Making Methods

Based on the investigation into current regulatory approval processes, a general process model was developed that described decision processes used in safety assessment as a prerequisite for operational approval. An influence matrix framework was also developed to represent decision-making regarding the influence of changes in proposed system behavior on risk. The framework is introduced in Chapter 4.

Three distinct approaches to performing safety assessment for operational approval are described using the framework in Chapter 5. These approaches include assessment to risk-based criteria through target levels of safety and risk matrices. The analysis is also conducted for assessment in comparison to a reference system.

1.6.3 Case Studies

Cases studies of past and pending air transportation system changes were performed to provide insight into the application of safety assessment processes to specific systems. Cases were selected which combined technical and procedural elements and introduced a change in the way operations were performed in the air transportation system.

The case studies were limited to those with sufficient available documentation of the safety assessment and safety case presented to regulators for approval. In some cases, direct documentation of safety analysis was available, while others had sufficient documentation in secondary literature. The cases studied are shown in Table 1-3. Six of the changes reviewed have been implemented and are operational. Two cases are pending approval.

Table 1-3: Case Studies Analyzed

No	Case	Implemented
1	Instrument Landing Systems (ILS)	1961
2	North Atlantic Organized Track System (NAT OTS)	1966-1981
3	Traffic Alert and Collision Avoidance System (TCAS)	1993
4	Precision Runway Monitor (PRM)	1997
5	Automatic Dependent Surveillance, Broadcast (ADS-B) Alaska Capstone	1999
6	EUR Reduced Vertical Separation Minima (RVSM)	2002
7	Automatic Dependent Surveillance, Broadcast (ADS-B) Segments I and II	(pending)
8	Unmanned Aircraft Systems (UAS)	(pending)

The documentation available for Reduced Vertical Separation Minima (RVSM) in Europe provided sufficient detail to apply the influence framework developed in the previous approach step. This allowed scoping decisions to be discussed in detail in the EUR RVSM case, using the influence framework in Chapter 7. The safety assessment process was examined for other cases,

and the analysis was used to identify key trends and challenges in safety assessment of each specific change. The analysis and discussion of the remaining 7 cases and additional aspects of RVSM is included in Appendix D.

1.6.4 Identification of Challenges and Implications for Future Air Transportation System Changes

Evidence from the previous analyses conducted was used to identify challenges in safety assessment and operational approval of future systems-level changes. These challenges are described and analyzed in Chapter 7.

2 Key Concepts and Literature Review

This chapter presents an overview and definition of key safety concepts used in this work. Alternate definitions will also be acknowledged and discussed when they differ significantly from those used in this work. First, key concepts related to safety as a property of events are defined. Next, key concepts related to the process of assessing safety are defined.

A review of the literature was conducted in the areas of safety in complex systems and system change processes, specifically focusing on air transportation systems. The literature review is presented following the definition of key concepts. This review of the general literature is separate from the safety regulatory policy and process documentation that was reviewed as a basis for description of current safety regulatory processes in the following chapter.

2.1 Operational Events and Safety

The goal of safety is to eliminate harm to things that society values. A system is said to be safe if it does not exhibit harm. For this work, safety is defined as freedom from harm to people and property. Prevention of harm to people and property is the basis of safety standards in air transportation. Therefore, safety is defined in this work as:

Safety: freedom from harm to people and property

It is common to define safety conceptually. There are alternate definitions of safety as an acceptable level of safety, which implies a threshold for which unsafe occurrences are tolerated (see e.g. [10, 11]). This alternate definition recognizes that it is impractical to expect perfect safety in an operational, safety-critical system.

Safety is often measured through its absence. An accident is an occurrence in the operation of a system that causes harm to people or property. Accidents are therefore unsafe occurrences.

Accident: an occurrence of harm to people or property in the operation of a system.

There can be different magnitudes of harm associated with occurrences. Differing magnitudes are defined by the measure of severity. Severity is typically defined through discrete categories of severity (e.g. minor, hazardous, catastrophic). Defining categories and criteria for severity is a policy decision that incorporates societal values regarding magnitude of harm. In air transportation safety assessment, adverse effects on people and property are typically used to define categories of harm in air transportation.

Severity: a measure of magnitude of harm.

The National Transportation Safety Board (NTSB), the U.S. federal agency responsible for investigating transportation accidents defines an accident as having a different level of severity than defined above: as death or serious injury or hull loss².

The concept of risk is frequently used in judging the safety of a system. Two definitions are presented here related to risk: risk as an event and risk as a measure. A risk event, which will be defined as a risk, is an adverse occurrence with associated harm. For example, when it is stated that operating an aircraft carries elements of risk, it is meant that there is the potential for something undesirable to occur, such as an accident. A risk event is a hypothesized occurrence used in evaluating the safety of the system. It can be an occurrence directly associated with harm to people or property. A risk event can also be an occurrence with an indicator of potential for harm, such as an increase in workload.

Risk: An occurrence with associated harm to people or property or with indicators of the potential harm to people or property

² In 49 CFR 830.2 [governing the NTSB] – Definitions, an accident is defined as any occurrence of death or serious injury of any person, or substantial damage to an aircraft that occurs in operation of the aircraft. Additionally, Boeing commonly reports accident statistics in the form of hull losses. This term originates in the insurance injury, indicating that the aircraft hull is damaged beyond repair and the accident is a total financial loss.

Risk events can be aggregated into a group by common factors. Risks can be grouped by severity of harm (e.g. fatal accidents, catastrophic accidents, etc). Risks can also be grouped by a common category of causality (e.g. controlled flight into terrain, runway overrun, etc [12]). Examining risks as groups can indicate common approaches to reduce their likelihood of occurrence, or can be used to judge the safety of a given class of events.

For any individual risk or grouping of risks, it is useful to define the level of risk. The level of risk, or risk level, measures the likelihood of occurrence of the risk event.

Level of Risk: a measure of the likelihood of a risk event

A hazard is defined in system safety to occupy an intermediate state between a set of potential initiating events and their harmful outcomes. In this work, a hazard will be defined as a set of conditions that could result in harm. This is consistent with common practice in civil aviation [11, 13] and military risk assessment processes [14]. Because it represents an intermediate state, for every hazard present in the operation of a system there can be several potential risks that can follow.

Hazard: A set of conditions of a system that could result in harm

2.2 Safety Assessment

Safety assessment is a structured process to evaluate the expected safety of a system. The process can be performed for a system which is either hypothetical or currently in operation, and techniques and methods used to characterize safety performance can vary.

Safety Assessment: a process for determining the expected safety of a system

There is often a need to define criteria for acceptable safety performance. These standard will be defined as *acceptability criteria*. Acceptability criteria have several forms. As examples, they can be in the form of a required process, an acceptable level of risk, or a measure of system performance.

Acceptability criteria/criterion: a criterion or set of criteria that define acceptable safety

In a strict sense, safety assessment is an analysis process for determining expected safety, and does not imply any action taken to address performance beyond those defined in acceptability criteria. In the assessment of a system, it is likely risk levels may exceed acceptability criteria. The process of addressing unacceptable levels of risk assessed - by deriving requirements for a system or changes to the system - will be defined as mitigation.

Mitigation: the process of addressing unacceptable safety performance of a system.

The associated requirements derived through safety assessment and mitigation to meet safety objectives will be defined here as safety-derived requirements.

Safety Derived Requirements: requirements derived through safety assessment to meet a safety objective.

2.3 Literature Review

The discussion of literature is organized by topic area. The first section describes relevant literature on the perception and communication of risk. The next section discusses literature related to accidents and safety. The following section focuses on new approaches to assessment of safety-critical systems. The next section describes literature relevant to change processes in air transportation system. The section concludes with current literature discussing safety assessment in air transportation, with some literature directly addressing expected challenges in future changes.

2.3.1 The Concept of Risk, Risk Perception, and Risk Communication

The concept of risk is the subject of a significant amount of scholarly work across multiple disciplines. Among other characteristics, studies have focused on the definition of key attributes of risk, how risk is communicated and perceived, and how risk is measured.

There is general consensus that the applicable concept of risk to technological systems is a relationship to danger or harm [15]. A further review of varying definitions of the concept of risk is provided by Thompson and Dean [16]. The authors classified risk definitions on a spectrum of contextualist and probabilist interpretations. As a probabilistic concept, risk is defined as a combination of probability and associated severity of an event. This approach was

common in early technological studies of risk, most notably those by Starr and Whipple [17]. In contrast, the contextualist interpretation holds that risk is determined by multiple factors, of which likelihood is only one among several. This view is common in psychological literature [18] [19].

In commercial air transportation, the probabilistic approach is common in characterizing risk. The NTSB reports annual accident rates by type of aircraft operation (e.g. general aviation, commercial airlines, etc [5].) Boeing reports hull loss occurrences categorized by an internationally-defined taxonomy [12].

Accidents invoke a phenomenon known as the social amplification of risk, as explained by Kaspersen [20]. This amplification of risk occurs primarily due to the response of the media, which amplifies the effects of one event in “ripples” to other areas of industry and society [20]. The amplification of risk perception through media coverage has been studied [21]. Commercial aviation accidents are generally perceived as more strongly related to risk as they typically result in multiple fatalities, typically occur near metropolitan areas, and are heavily covered by the media [22]. Risk perception is also related to the policy question of acceptable risk, studied extensively by Fischhoff, et al. [23].

2.3.2 Accident Causality and Safety

Early examination of safety in complex sociotechnical systems was performed by Rasmussen [24], laying the foundation for several related areas of investigation into the many factors that contribute to accidents in complex systems. Normal Accident theory was proposed by Perrow [25] to describe system accidents as the result of complexity and tight coupling in systems. In addition, Reason [26] has examined organizational factors and structures that contribute to accidents. High reliability organizations [27] are a formalism that also describe organizational management of complex systems.

Increasing focus has been applied to addressing the role that organizational factors and conditions contribute to the safety of systems. Hollnagel, et al. [28] have defined the concept of resilience to formalize the analysis of organizational structures and conditions and how they respond to emergent safety issues.

Many best practices related to organizational response to accidents have been incorporated into guidance on Safety Management Systems in industry and by Regulators [11, 29]. Safety Management Systems promote a safety culture and best practices to dynamically manage safety in organizations.

2.3.3 New Approaches to Safety Assessment in Complex, Safety-Critical Systems

Traditional approaches to safety-assessment are widely established and utilized. Fault tree analysis/ event tree analysis (FTA/ETA), failure hazard analysis (FHA), and failure modes and effects analysis (FMEA) were initially used to describe failure modes of mechanical systems. The basic cause-hazard-consequence method of safety assessment has been extended to describe human, software, and organizational failures. The use of hazard assessment is well established in air transportation system standards on safety assessment by the FAA [11] and others [30, 31]. A review of current methods and models of civil air transportation safety can be found in [32].

There is a recognition that extending the failure probability approach to complex systems involving human and organizational failures becomes increasingly difficult as the complexity grows and failures shift from mechanical failures to human and organizational failures. One new approach has been to assess the influence of organizational factors on safety through system dynamic modeling by Leveson [33]. This approach focuses on the general influence of organizational structure and authority on risk. This approach does not, however, seek to quantify risk or provide decision guidance on system configurations to reduce risk. Marais has extended this approach [34] by identifying and understanding archetypes of organizational influences on risk.

A separate approach to safety assessment involves quantifying expert judgment of event probabilities. These subjective probabilities can be structured as transition likelihoods for physical events, and arranged in Petri nets. This allows complex behavior to emerge from simple descriptions of the actions of many agents as so-called agent-based modeling. This approach originated at NLR with Blom and integrated into the TOPAZ tool [35]. Another approach to elicit expert probabilities to on risk influences of different interventions. This approach is known as a Bayesian Belief Network (see e.g. [36]).

As systems have become more complex, the underlying assumptions and justifications in assessing change have also become more numerous. To address the often complex nature of a safety case, Goal Structuring Notation (GSN) provides a method to organize the arguments in support of a safety case [37]. The purpose of GSN is to determine if logically consistent justifications are made in the safety analysis of a system, or to determine the required reassessment if an aspect of a safety case comes under question.

Software poses a separate set of challenges in safety assurance. The National Academy of Science recently examined software challenges and conclude that additional evidence-based approaches are need to assure software integrity [38]. To this point, software standards have been focused on integrity assurance through assurance on the development process [39]. Some approaches, such as formal methods use structured mathematical theory to assure implemented software performs as specified, but are currently limited to simple functions performed by software [38].

2.3.4 Air Transportation Change Processes

In general, it is difficult to achieve system transition in air transportation. Due to the complexity of the system, and its multi-stakeholder nature, change is typically a long and complicated process, as shown by Mozdzanowska [40]. Safety catalytic events tend to drive safety-related changes for the system, but it is not clear what will be a parallel driver for capacity-driven system modernization. The delivery of cost and benefit to stakeholders has also been investigated [41].

Several studies have highlighted issues in FAA safety approval processes generally, and for specific systems. RTCA Task Force 4 was charged in 1999 with examining the FAA certification processes for new systems [42]. The task force found several deficiencies related to systems engineering, dealing with emerging technology, coordinating management processes, and understanding human interactions with systems. GAO has also reviewed coordination processes for new technology, and found insufficient coordination between processes for certification of airborne equipment and approval of ground equipment [43]. Concerns have also been highlighted with the organizational structure of the FAA as both regulator and operator in a review by the Brookings Institution [44].

GAO has examined several cases of delayed approval, or of specific problems in specifying new technologies. One example is the Wide Area Augmentation System (WAAS) [45]. Other studies have highlighted similar persistent issues in other programs, such as Controller-Pilot Datalink communications (CPDLC) [43]. In addition, Hansen examined the air carrier oversight process, noting increasing trends toward risk-based oversight [46]. The DOT inspector general's office has audited FAA's Aviation Safety Action program and found deficiencies in the use of risk-based data [47]. Downer [48] studied issues in assurance bases and test criteria from a sociological standpoint, primarily through reviewing airworthiness criteria.

2.3.5 Challenges in Future Air Transportation Safety

A growing body of literature motivates the need to identify precursors to accidents. Future work is likely to build fundamentally on the theory of parameter identification of distributions based on a limited number of observations, described by [49]. Experienced safety assessors, such as Fowler and Brooker have identified research challenges in safety of new air traffic control systems [50] [51]. The authors highlight the need to identify precursors and utilize less reliability-focused methods, extending analysis to organizational and other systems-level factors [52].

3 Current Safety Regulatory Processes and Policies in US Air Transportation

This chapter provides a summary of current safety regulatory processes and policies in air transportation. This includes both approval processes and standards for various components of the air transportation system as well as supporting safety assessment processes. The investigation is focused on U.S. Federal Aviation Administration (FAA) policies, processes, and procedures. FAA policies are similar to those used in other developed nations. Where it is relevant to current FAA policy, international policies on approval are also highlighted and explained.

The chapter begins with an overview of the components of the air transportation system and a discussion of relevant policies regarding their approval. Additionally, the distribution of functionality across air transportation system components in systems-level changes is further emphasized. After this introduction, a model of the assessment and approval processes for changes with distributed functionality is introduced, which has been created based on the investigation of current safety regulatory policies and practices. This model describes the structure and sequence of specific approval processes and standards for individual components of a distributed change.

Following the model, background is provided on the general safety assessment processes used to determine required performance at a systems-level. This discussion focuses on the general FAA process of Safety Risk Management, and its similarity to safety assessment approaches used in industry and advisory committees to derive requirements for a systems-level change. After the discussion of safety risk management, approval processes for specific components of the air transportation system will be described. This discussion provides background on the varied approaches used to assure the safety of air transportation components, and highlights key differences between processes.

The chapter concludes with a brief overview of other processes present in the air transportation system that affect safety. These include oversight and monitoring processes that are beyond the scope of this work.

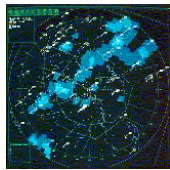
3.1 Air Transportation System Components

The air transportation system consists of multiple interacting components that serve to safely transport passengers and cargo. These components are both physical and virtual: including aircraft and ground-based infrastructure as well as procedures. Each of these components can be considered a system in itself, with further decomposition to components. As an example, an aircraft can be described as one component of the overall air transportation system. An aircraft can also be described as a system, with the components of wings, passengers, avionics, etc. A systems-level change is composed of distributed functionality across air transportation system components of aircraft, air traffic control, etc. that will be described in more detail here. This is consistent with describing these objects as components of the overall air transportation system. Components of the air transportation system outside of the boundary of the proposed change will be referred to as being part of the external system.

A summary of the components of the air transportation system and relevant policies is shown in Figure 3-1, which has been updated and adapted from [42]. On the airborne side, *aircraft* are defined as “contrivances designed to fly in the air” [53]. Aircraft include a wide range of types – hang gliders, ultralights, unmanned aircraft systems, propeller, jet transports, helicopters, etc. Unless otherwise noted, when aircraft are referenced in this work, it is generally assumed that these are conventional airplanes such as commercial airliners, business jets, and recreational aircraft. Major subcomponents of aircraft are also certified separately, known as *subcomponents or parts*. These include engines and propellers. Avionics also fall under this category, which are electronic equipment installed in aircraft.

Air Traffic Control Systems

(Acquired systems: e.g. hardware)



Acquisition Management System (AMS) Policy

Safety Risk Management Guidance for System Acquisitions (SRMGSA)

Configuration Management Policy (Order 1800.66)

Pilots

(Pilot certificates, ratings, medical certificates)



Part 61: Certification of Pilots, Flight Instructors, and Ground Instructors

Air Traffic Controllers

(Credentials)



Order 8000.9: AOV Credentialing

Aircraft

(design of aircraft type)

Part 23: Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes

Part 25: Airworthiness Standards: Transport Category Airplanes

(also rotorcraft, balloons, etc.)



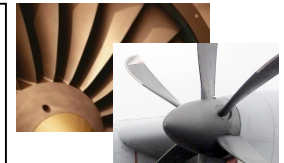
Aircraft Components

(engines, propellers, avionics)

Part 33: Airworthiness Standards: Aircraft Engines

Part 35: Airworthiness Standards: Propellers

(also, maintenance and avionics)



Airports

(serving commercial operations)



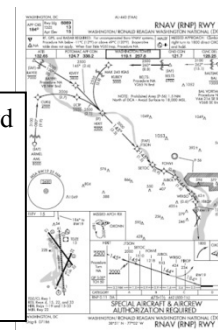
Part 139: Certification of Airports

Procedures

(e.g. terminal instrument procedures)

Part 97: Standard Instrument Procedures

Order 8260.3B: TERPS



Aircraft Operators

(e.g. air carrier operating certificates)

Part 121: Operating Requirements: Domestic, Flag, and Supplemental Operations

Part 135: Operating Requirements: Commuter and on Demand Operations and Rules Governing Persons on Board such Aircraft



Figure 3-1: Air Transportation System Components Requiring Safety Approval

(Adapted from [42])

Also in the airborne category, aircraft are operated and maintained by *airmen*. Pilots are the most common category of airmen. However, the category also describes flight engineers, navigators, dispatchers, mechanics, and repairmen. In this work, the flight crew will generally refer to the pilots of aircraft. For certain types of operations, there are organizations created to operate single or multiple aircraft. In these cases, the organizations are referred to as *aircraft operators*. Commonly, these organizations are referred to as airlines, and there are several different categories depending upon the type of operation that will not be described in detail here.

There are also components of the air transportation system that function as supporting infrastructure, which facilitate the operation of the system. For example, *Air Traffic Control* (ATC) relies on ground and satellite-based surveillance, navigation and communication to support separation of aircraft and access to resources. Air traffic control is performed by *air traffic controllers*. Controller tasks are supported by hardware and software-based decision support systems, displays, and automation. There are other physical components of ground infrastructure. These include *airports* – locations for aircraft to takeoff and land. Space-based infrastructure, such as the Global Positioning System (GPS), and communication satellites also support the operation of the system.

The functioning of the air transportation system is based on a common set of *procedures*. These procedures, generally referred to as “rules of the air” define protocols for operation under different conditions. Specific operational procedures certified for use by airlines and pilots, and controllers are trained and conduct defined procedures. Specific navigation procedures, such as routes for arrival and departure to airports are also used.

3.2 Safety Assessment and Operational Approval of Distributed Capabilities

The Investigation of current safety regulatory practices was used to construct a representation of the general process of assessment and approval of systems-level capabilities. This is shown in Figure 3-2 and discussed in this section. In the figure, an overall system or proposed change is highlighted in grey. Elements of a change are divided into the categories of aircraft-based, procedural, and infrastructure components. Other objects and processes are defined in the legend.

The steps preceding operational approval generally fall into the categories shown at the top of the figure. A system description process takes a desired capability in the system and defines the artifacts that are required to achieve that capability. These artifacts constitute the proposed change, and can include flight crew procedures, aircraft avionics, operational procedures, and infrastructure (air traffic control, surveillance, and communication infrastructure). In addition, the applications performed by the proposed change are also part of the system description. Examples of applications are airborne self-separation or midair collision conflict avoidance. At this stage, the description of the proposed change is usually captured in a concept of operations, which describes both the components of the change, and how it will be operated in the air transportation system.

The proposed change is assessed to safety standards at a system level through modeling and analysis. This process is safety assessment. Safety assessment is one basis for the general process of specification development shown in the figure. Specification development leads to detailed specifications from the description of artifacts of the proposed change. Specifications can be decomposed to individual components of the change, as shown. There can also be specified required performance at a systems level.

This work is focused on the processes of safety assessment at a systems level. It is at this stage of the system's life cycle where significant flexibility exists to incorporate changes to the system. Standards derived at this stage are also used in downstream approval processes.

The process of incorporation of safety-derived requirements occurs after detailed specification development. In this process, detailed specifications derived through safety assessment are incorporated into existing approval processes. This step is necessary due to existing divisions of responsibility and separate processes for approval by component. In the figure, orange ovals represent the policies governing each individual component, through which specific requirements will be enforced. Based on these standards, the resulting types of requirements are shown in boxes following each process.

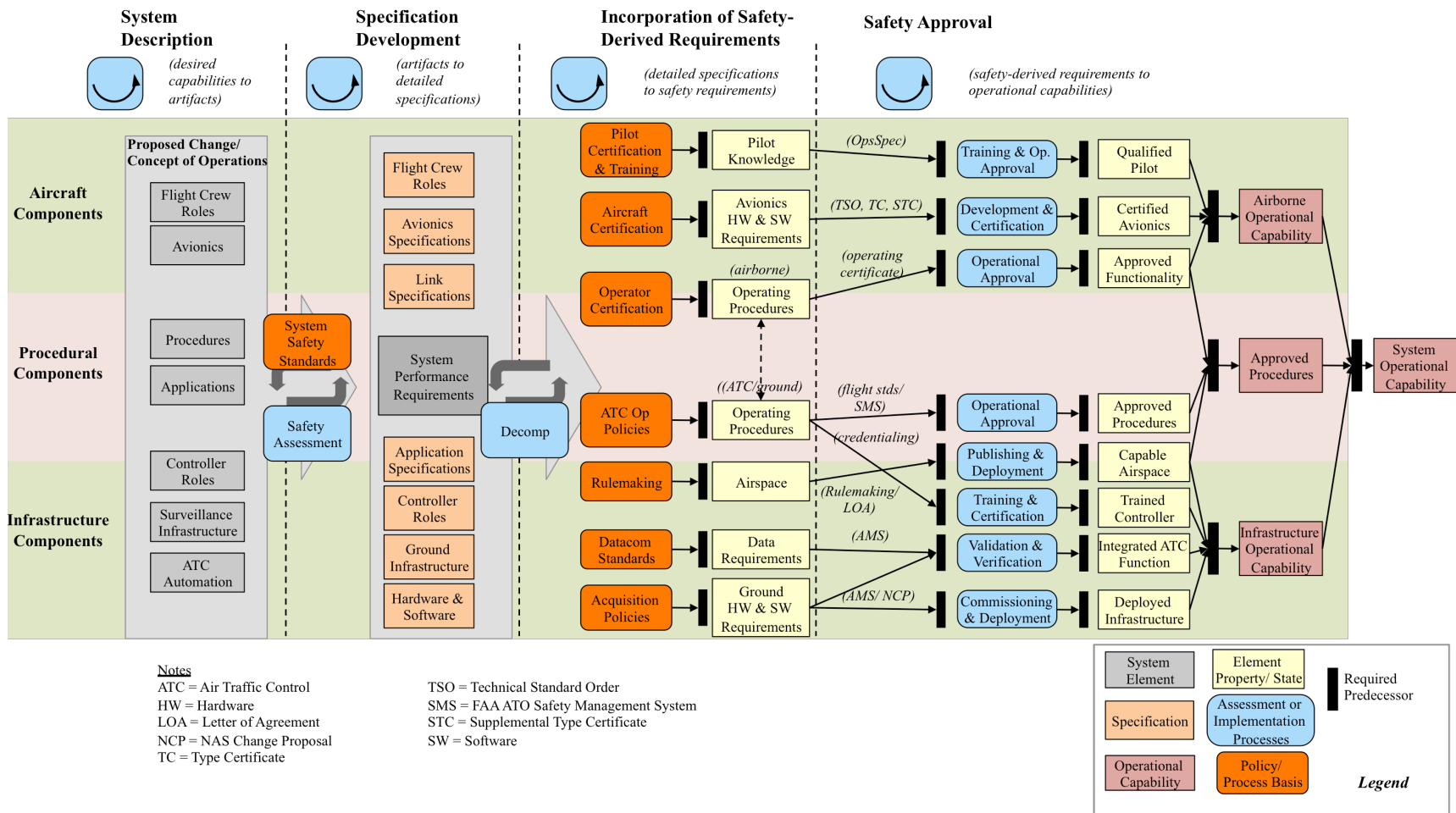


Figure 3-2: Processes Supporting Safety Operational Approval of a Systems-Level Change

There are subtle but important differences between airborne and ground capabilities in how new requirements are integrated into existing policies and processes. In general, for aircraft-based capabilities, performance is certified to minimum standards specified by regulation. Regulations also govern how the certification process is performed. For certain system elements (e.g. avionics), regulations or regulatory guidance (e.g. advisory circulars) establish minimum performance standards for the specific element. Safety-derived requirements are incorporated as standards for equipment. As an example, if a specific flight crew or airline will utilize procedures, they are approved as part of the carrier's operating certificate. Changes made to operating rules require a notice of proposed rulemaking.

For ground-based systems, safety-derived requirements are incorporated through systems engineering processes of validation and verification to internal regulatory or procurement standards. This is due to the historical practice of acquiring ground-based systems, where a system as a whole is built to specifications and acquired and implemented by the operator. By this process, acquisition policies establish methods for including safety-derived requirements along with other general requirements, which are approved in program milestones.

Specifics of procedures may differ depending upon whether they support an airborne capability or infrastructure capability, but the general function performed is common to the two capabilities, shown by the dashed line connecting airborne and ATC/ground operating procedures. Procedures are decomposed and approved separately for airborne and infrastructure domains.

As a final step, safety approval processes are conducted for the specific artifacts or procedures that compose the proposed change. The specific process used to achieve this is labeled on the arrows from requirements to approval processes. The completion of component safety approval processes result in an approved artifact or procedure. Once all elements in a capability are approved, the capability is operational. This is shown as the airborne operational capability, procedural operational capability, and infrastructure operational capability. For some changes, one of these capabilities in isolation may be sufficient for an application. However, when the change is distributed across air, ground and procedural capabilities, all are necessary to achieve an operational capability in the system.

This section has provided an overview of the general flow of assessment and approval processes to achieve an operational capability. In the following sections, the detailed policies and processes for approval of individual components will be described.

3.3 Safety Assessment

Safety assessment is the process of examining safety-related behavior of a system by: defining potential hazardous states, determining if hazards meet defined safety objectives, and correcting any deficiencies that do not satisfy safety objectives. Safety assessment is a key process supporting safety approval decisions across a range of air transportation system components. Its extensive use in setting systems-level safety performance requirements merits a detailed discussion in this section. Within FAA operational approval documentation [11], safety assessment is referred to as Safety Risk Management (SRM).

There are several forms of analysis within the category of safety assessment. When examining failures of components of a system, the process is referred to as Fault Hazard Analysis (FHA). When performed early in a system's life cycle, the safety risk management process is a Preliminary Hazard Analysis (PHA). There are many other individual techniques used to perform safety assessments that are risk management processes, but will not be discussed in detail here.

The FAA requires safety assessment to be performed for any change to the air transportation system that could significantly impact safety. ATO SMS policy requires safety assessment for significant changes to airspace, procedures, or Air Traffic Control systems [11]. In addition, several aerospace design standards incorporate guidance on determining system performance requirements to meet acceptable risk levels. RTCA publishes guidance on system design processes for air traffic services supported by data communications [30]. Other safety assessment guidance includes SAE ARP 4761 [31], the FAA System Safety Handbook (which was primary guidance prior to SMS implementation) [13], Mil-STD-882 [14], and FAA acquisition guidance [54]. Risk matrices are also used in European safety standards (e.g. ESARR4 [55]) and other safety-critical industries [56].

In more detail, the four steps in the risk management process described in the ATO SMS [11] are:

- 1) Describe the system: Functional relationships within the system are described, as well as the boundary of the system and its relationship within an external system in which it operates.
- 2) Identify hazards: through two different processes, potential hazards are identified, and a set of hazards expected in operation of the system is obtained. Backward identification considers causes of unsafe states in the system, and then infers which general hazardous states the system could arrive at. Forward identification considers potential outcomes (such as a midair collision), and then deducts what hazardous states could precede these outcomes.
- 3) Analyze and Assess Risk: Using a model of the system, existing risk controls are identified, and then the potential risk of each hazard is assessed through a system model. The system model can be a quantitative model, or can be implicitly held by assessors to arrive at qualitative judgments. Based on the combination of severity and likelihood, risks are ranked in a risk space, and prioritized for potential interventions.
- 4) Treat Risk: Once risks have been ranked and categorized, they are treated by applying mitigations or requirements to reduce risk to an acceptable level. It is usually assumed that these treatments are independent of the previous behavior of the system. The new “mitigated” system does not need to be re-analyzed through the risk assessment process. In the case of design requirements, models of the system may be redone with new design requirements [11].

Acceptability Standards. The FAA ATO SMS also defines acceptability criteria in risk management. The criteria used for acceptability are defined in a risk matrix, shown in Figure 3-3. The matrix is organized with levels of risk severity along one dimension, and categories of likelihood (risk level) along the other dimension. A given risk is assigned a ranking based on its location in the matrix, which is function of its risk level and severity. For the ATO SMS risk matrix, there are three risk rankings: high, medium, and low. Mitigation and approval requirements differ depending upon the risk ranking. As an example, risks with a risk ranking of “high risk” are unacceptable without mitigation [11], and mitigation measures are required to be approved by the air traffic oversight (AOV) branch for risks initially ranked as high. In the ATO SMS process, risks are identified for each hazard analyzed, and it is typically the worst credible risk that is ranked in the risk matrix.

Severity Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

High Risk
Medium Risk
Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

Figure 3-3: Risk Matrix Classification of Risk [11]

Five categories of severity range from *no safety effect* to *catastrophic*. As the severity level increases, the magnitude of harm associated with the risk increases. As an example, hazardous severity events on aircraft are characterized by a small number of severe or fatal injuries. Catastrophic level events result in multiple fatalities or hull losses (the destruction of an aircraft fuselage). Severity of harm is classified depending on general effects, and specific effects on the function of air traffic control and the flying public (flight crews and passengers). The categories of severity and associated descriptions from the FAA ATO SMS [11] are shown in Table 3-1. Some categories do not directly have fatality or injury harms associated with them. As an example, major severity ATC events are characterized by a reduction in separation due to a low or moderate severity operational error, or significant reduction in ATC capability. Neither of these criteria directly describes harm to passengers. Instead, they indicate an increased potential for harm.

Table 3-1: ATO SMS Severity Definitions [11]

Effect on:	Hazard Severity Classification				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
General		Does not significantly reduce system safety. Required actions are within operator's capabilities. Includes (see below):	Reduces the capability of the system or operators to cope with adverse operating conditions to the extent that there would be a (see below):	Reduces the capability of the system or the operator's ability to cope with adverse conditions to the extent that there would be a (see below):	Total loss of systems control such that (see below):
Air Traffic Control	Slight increase in ATC workload	Slight reduction in ATC capability, or significant increase in ATC workload	Reduction in separation as defined by a low/moderate severity operational error (as defined in FAA Order 7210.56), or significant reduction in ATC capability	Reduction in separation as defined by a high severity operational error (as defined in FAA Order 7210.56), or a total loss of ATC (ATC Zero)	Collision with other aircraft, obstacles,
Flying Public³	No effect on flight crew Has no effect on safety - Inconvenience	Slight increase in workload Slight reduction in safety margin or functional capabilities Minor illness or damage Some physical discomfort	Significant increase in flight crew workload Significant reduction in safety margin or functional capability Major illness, injury, or damage Physical distress	Large reduction in safety margin or functional capability Serious or fatal injury to small number Physical distress/excessive workload	Outcome would result in: Hull loss Multiple fatalities

Definitions of risk levels in the ATO SMS are defined as shown in Table 3-2 [11]. Both quantitative and qualitative definitions of likelihood are defined. Five categories of risk levels range from *frequent* to *extremely improbable*. Each category increases the quantitative description of likelihood by two orders of magnitude, from 10^{-3} events/hr to 10^{-9} events/hr.

Risk level criteria are commonly referenced for hazardous and catastrophic events. By referring to Figure 3-3, it may be noted that the minimum acceptable level of risk for a catastrophic event is extremely improbable. This translates to a quantitative probability of 10^{-9} events/hr. Similarly, for hazardous severity events, the probability is 10^{-7} events/hr.

FAA advisory circulars for aircraft systems, AC 23.1309 [57] and 25.1309 [58] also present risk-matrix criteria as methods for assessment of failure conditions of installed systems. These methods are not addressed in this work, as they are a means of assessing required reliability of aircraft subsystems.

³ For more information regarding these definitions, refer to FAA Advisory Circular 25.1309-1A, *System Design Analysis*, 06-21-88. [footnote in original]

Table 3-2: ATO SMS Likelihood Definitions [11]

	NAS Systems			Flight Procedures	ATC Operational	
	Quantitative	Qualitative			Per Facility	NAS-wide
		Individual Item/ System	ATC Service/ NAS Level System			
Frequent	Probability of occurrence per operation/ operational hour is equal to or greater than 1×10^{-3}	Expected to occur about once every 3 months for an item	Continuously experienced in the system	Probability of occurrence per operation/ operational hour is equal to or greater than 1×10^{-3}	Expected to occur more than once per week	Expected to occur more than every 1-2 days
Probable	Probability of occurrence per operation/ operational hour is less than 1×10^{-3} , but equal to or greater than 1×10^{-5}	Expected to occur about once per year for an item	Expected to occur frequently in the system		Expected to occur about once every month	Expected to occur about several times per month
Remote	Probability of occurrence per operation/ operational hour is less than or equal to 1×10^{-5} but equal to or greater than 1×10^{-7}	Expected to occur several times in life cycle of an item	Expected to occur numerous times in system life cycle	Probability of occurrence per operation/ operational hour is less than or equal to 1×10^{-3} but equal to or greater than 1×10^{-7}	Expected to occur about once every year	Expected to occur about once every few months
Extremely Remote	Probability of occurrence per operation/ operational hour is less than or equal to 1×10^{-7} but equal to or greater than 1×10^{-9}	Unlikely to occur, but possible in an item's life cycle	Expected to occur several times in the system life cycle	Probability of occurrence per operation/ operational hour is less than or equal to 1×10^{-7} but equal to or greater than 1×10^{-9}	Expected to occur about once every 10-100 years	Expected to occur about once every 3 years
Extremely Improbable	Probability of occurrence per operation/ operational hour is less than 1×10^{-9}	So unlikely that it can be assumed that it will not occur in an item's life cycle	Unlikely to occur, but possible in system life cycle	Probability of occurrence per operation/ operational hour is less than 1×10^{-9}	Expected to occur less than once every 100 years	Expected to occur less than once every 30 years

3.4 Safety Approval Processes by Air Transportation System Component

The previous section described the safety risk management process used by the FAA in evaluating systems-level changes. Previously, this process was placed in the context of the more specific safety approval processes for each component of the air transportation system. This section presents a more detailed discussion of safety approval processes by component of the air transportation system.

Approval processes will be described in the following order: aircraft and airborne equipment certification; airmen and air traffic controller certification; operator certification and operational approval; and airspace procedure design and approval. Following this, approval processes are for specific procedures, programs, or aspects of a systems-level capability are discussed. These include: separation standards and surveillance systems; ground-based programs; and software and complex electronic hardware.

3.4.1 Aircraft and Airborne Equipment Certification

The FAA certifies aircraft and associated components through several certification processes. Aircraft airworthiness is certified through an *airworthiness certificate*. A *type certificate* is “issued by the FAA when the applicant demonstrates that a product complies with the applicable regulations [59].” This certificate is issued for the general design of one type of aircraft following an extensive set of review procedures between the FAA and the applicant [59]. Each individual aircraft is issued an *airworthiness certificate* for a given type design. Airworthiness of individual aircraft of a type is guaranteed through a quality control process called *conformance*. Type certification of an aircraft encompasses all subcomponents within the type design, including the structure of the aircraft, avionics, and any parts used in the aircraft. It also dictates other products that are approved for use on the aircraft, such as engines and propellers.

A type certificate is issued to an established regulatory basis, which includes applicable *airworthiness standards*, any agreed-upon deviations from standards and appropriate measures, and process documentation. Airworthiness standards are published in FAR Parts 23, 25, 27, 29, 31, 33, and 35. There are exceptional categories of airworthiness certificates that can be issued without type designs, such as experimental airworthiness certificates for research and development [60] and amateur-built aircraft. There are also classes of aircraft, such as ultralights [61], that do not require airworthiness certification prior to operation. Minor changes to type certificates can also be obtained through a *supplemental type certificate*. Supplemental Type Certificates (STCs) are used for changes to the aircraft not included in the original type certificate, such as repairs to structure. They are also used to certify changes to major components that are updated from the original type certificate, ranging from cockpits to wheel assemblies. The process for application and issuance of certificates for aircraft and parts is also established by specific regulation⁴.

The FAA also issues *production certificates* [62] to applicants. A production certificate is a form of approval to manufacture a given type design or part. Holding a production certificate expedites the issuance of airworthiness certificates for individual aircraft.

⁴ FAR Part 21, Certification Procedures for Products and Parts

Major subsystems of such as propellers are subject to separate sets of regulations that prescribe their required minimum performance⁵. Separate companies from airframe manufacturers typically manufacture propellers and engines.

For subcomponents of aircraft, there are processes for approval of parts of aircraft that can be installed or replaced when not covered by the type certification of the aircraft. These include Supplemental Type Certificates (STC), Technical Standard Orders (TSO), and Parts Manufacturing Approval (PMA). STC approval was discussed above, and is generally granted to an applicant for a major change to a type certificate [63]. PMA is granted to an applicant from the FAA as design and manufacturing approval for a replacement part for type certified aircraft [63].

A TSO is different from a PMA, although it serves a similar function, to certify the design and artifact for a replacement part. The basis for a TSO is a “minimum performance standard for specified articles [64]” Thus, a technical standard order approval is to an FAA-published specification of performance. TSOs contain functional requirements, certification process requirements, and testing requirements to certify given articles. It does not allow for approval of installation or use of the avionics [65].

Processes for approval of aircraft parts require the FAA to publish associated orders or advisory circulars, which dictate their minimum performance. Creation of these standards is abbreviated compared to the process for creating new regulations, but it also provides a level of standardization apart from detailed review of an entire aircraft design. However, it has been found that TSOs are increasingly being used for more complex avionics [42]. Therefore defining requirements for TSOs requires more effort than in the past.

3.4.2 Certification of Airmen and Credentialing of Air Traffic Controllers

The FAA is certifies airmen and other flight crewmembers that operate aircraft, instruct others in operation, or perform maintenance. In general, certification requires completion of a specified training program and milestones, passage of knowledge tests, medical examination and

⁵ FAR Part 33 - Airworthiness Standards for Engines, and FAR Part 35 – Airworthiness Standards for Propellers

certification, and practical examination, among others⁶. To maintain privileges of some airmen licenses, there are also recurring requirements for continued experience (called currency requirements).

Specifically for pilots, certification privileges are categorized along several divisions. A pilot certificate allows a pilot to operate under Visual Flight Rules (VFR), a set of defined weather conditions that allow for visual navigation, detection of other air traffic, and landing. A separate rating, known as an instrument rating, is required to operating an aircraft under Instrument Flight Rules (IFR).

Pilot licenses can give the privilege to operate aircraft by category, which give a pilot an ability to operate broad classes of aircraft. Categories are typically defined by number of engines and type of airplane (land, seaplane, glider, balloon). As aircraft become more complex, it may be necessary to be “checked out” and hold a rating in a specific airplane type. This is required for aircraft above 12,500 lb. or turbine powered. A type rating gives the privilege to operate a specific aircraft by type.

Licenses are also granted at several levels, ranging from student pilot to air transport pilot. Levels provide different classes of privileges or, conversely, limitations. As an example, a commercial pilot can carry passengers for compensation or hire, while a private pilot is limited only to sharing the cost of operation with passengers. Pilots can also earn ratings allowing them to instruct other pilots.

Some types of aircraft do not require a private pilot certificate to operate. Ultralights require only a driver’s license (except for additional requirements in some states), while sport pilot certificates are granted with an abbreviated training process and less stringent medical requirements. These classes of aircraft are also typically no certified to the same level of airworthiness (as discussed above) as other classes of aircraft.

Air Traffic Controllers are required to pass an FAA-approved training program, most commonly the FAA Academy in Oklahoma City (there are also processes for abbreviated training for

⁶ FAR Part 61, Certification: Pilots, Flight Instructors, and Ground Instructors; FAR Part 63: Certification: Flight Crewmembers Other Than Pilots; FAR Part 64: Certification: Airmen Other Than Flight Crewmembers.

military air traffic controllers, and other authorized training centers). Initial training is combined with an apprenticeship process at operational centers. Initial controller coursework focuses on general knowledge of airspace, weather, and aircraft performance. Next, controllers learn procedures for their functional position through a combination of classroom instruction and simulator training [66]. Following academic work, controllers are then trained on the job at their assigned air traffic control center. The entire process takes approximately five years [66].

With the creation of the Air Traffic Oversight Branch (AOV), Air Traffic controllers are “credentialed” based on a completion of a set training process, and proficiency at a specific facility [67]. This was made as an effort to provide more structured regulation of Air Traffic Operations.

Other personnel engaged in safety-critical support activities are also certified, such as airway facility maintenance technicians to internal FAA standards [68] after completing required training.

3.4.3 Operator Certificates and Operational Approval

Aircraft that are certified or meet other approval requirements and flown by licensed pilots, have implicit approval to operate under General Flight Rules, FAR Part 91 [42]. The FAA additionally regulates operators who perform routine carriage of commercial passengers, or scheduled operation. These organizations are required to be certified, through *operator certification*. Specific procedures conducted by the operators are authorized through *operational approval*.

There are different classes of operating certificates depending upon the type of operations conducted by the airline⁷. Generally, certification requirements become more stringent the more

⁷ FAR Part 121 – Operating Requirements: Domestic, Flag, and Supplemental Operation

FAR Part 125 – Certification and Operations: Airplanes Having a Seating Capacity of 20 or More Passengers or a Maximum Payload Capacity of 6,000 Pounds or More; And Rules Governing Persons on Board Such Aircraft;
FAR Part 129 – Operations: Foreign Air Carriers and Foreign Operators of U.S.-Registered Aircraft Engaged in Common Carriage

FAR Part 133 – Rotorcraft External-load Operations

FAR Part 135 – Operating Requirements: Commuter and On Demand Operations and Rules Governing Persons on Board Such Aircraft

FAR Part 136 – Commercial Air Tours and National Parks Air Tour Management

FAR Part 137 – Agricultural Aircraft Operations

similar an airline is to common carriage of commercial passengers. There are several requirements to receive and maintain operating certificates: including maintenance, operating procedures, pilot training, and safety-based quality control requirements. *Oversight* of operating certificates are conducted to ensure continued compliance with FAA regulations by certificate-holders [46]. The process primarily involves structured audits by FAA Aviation Safety Inspectors [69].

Even if certified avionics are installed, to use the functions of the avionics, an air carrier requires *operational approval* from the FAA to utilize the set of avionics for a given function. This operational approval is granted to certificate-holders through appropriate sections of an Operations Specifications, or OpsSpec [69]. The relevant operational capability is approved as long as the carrier can satisfy provisions on pilot training, aircraft and avionics types used, and internal safety oversight functions. The FAA maintains standard OpsSpecs to expedite approval of different capabilities [69], but operational approval of new capabilities can be a lengthy process while capabilities are defined.

3.4.4 Airspace Procedure Design & Approval

The FAA division responsible for establishing instrument and visual flight rules, as well as oversight of air carrier operations is the Flight Standards Service (with the internal FAA designation of AFS). Part of AFS responsibility is to design and certify terminal and en-route flight procedures.

Instrument flight procedures are used to link ground-based navigational aids with aircraft capabilities to safely direct aircraft to landing and upon departure. As such, their design and certification heavily influences safety of aircraft. AFS sets the standards for design, review, approval, and publication of instrument approach and departure procedures in the terminal area, published in the United States Standard for Terminal Instrument Procedures (TERPS) [70], an internal FAA policy, and in Federal Regulation⁸. TERPS contains guidelines for approaches using different capabilities, as examples: Lateral Precision, Vertical Guidance (LPV) approaches via the Wide Area Augmentation System (WAAS), and Required Navigation Performance (RNP). As new approach capabilities are implemented in the system, Flight Standards

⁸ FAR Part 97 – Standard Instrument Procedures

determines appropriate criteria for approach procedure design to accommodate additional performance capabilities. AFS is also responsible for certifying automated procedure development software [71]. Once a procedure has been designed and published, it must be verified in flight tests by Flight Inspections, Central Operations (FICO) before receiving operational approval [69].

In addition to terminal instrument flight procedures, other procedures in air transportation are subject to approval by AFS. These include: minimum enroute altitudes [72], Category I, II, and III ILS approach and landing procedures, evaluation of proposed obstructions for impact on procedures, [71] and approval of letters of agreement that impact flight procedures [73].

3.4.5 Separation Standards & Surveillance System Performance

ICAO publishes guidance methods for determination of airspace separation minima [8]. The guidance emphasizes methods for evaluating safety of proposed changes to airspace or separation minima, enabled by Air Traffic Management Technologies. This guidance has been applied for changes in oceanic separation standards and by the FAA in evaluating ADS-B separation standards and implementation of RVSM.

There are two methods that ICAO recognizes for safety assessment of a proposed change in separation - *comparison with a reference system*⁹ and *evaluation of system risk against a threshold*. In the comparison to a reference system approach, the proposed system is analyzed relative to the performance of a similar system that has already been judged to be acceptably safe. The proposed system must perform equally or better to the reference system in identified measures of performance. In evaluating against a threshold, the modeled risk of a system must be equal to or below an established target level of safety (TLS).

⁹ The ICAO-defined *comparison with a reference system* approach is a subset of more general equivalence-based approaches that set requirements based on performance measures of a comparable system.

The minimum stated requirements for application of the reference system approach are:

- a) separation minima must not be less in the proposed system than in the reference system;
- b) proposed means of communication and surveillance must be no worse in terms of accuracy, reliability, integrity, and availability than those of the reference system;
- c) frequency and duration of the application of minimum separation between aircraft must not be greater in the proposed system than the reference system
- d) navigation performance (typical and non-typical) of the population of aircraft should be no worse in its effect on collision risk, in any dimension, than that of the aircraft in the reference system.

It may be noted that separation minima must not be less in the proposed system than the reference system. Therefore the reference system approach cannot be used to reduce separation beyond that established in current operation.

The process for comparing performance to a reference system considers several properties of the airspace dictated by ICAO. These include “the effect of changes along each factor must be shown to be equal or safer, or tradeoffs between factors must be evaluated” and “the effectiveness of TCAS may not be considered as a mitigation in the safety case [8].”

Evaluation of risk against a threshold involves identification of hazards and modeling of their severity and likelihood. Qualitative modeling is possible, but quantitative modeling through a collision risk model is usually performed. ICAO recommends several possibilities for a target level of safety that have been used in past changes [8].

3.4.6 Ground-Based Equipment and Programs

Ground-based systems fall under the technical category of “air navigation facilities” [42]. The FAA is empowered to define performance characteristics for air navigation facilities, and to deploy to meet air transportation needs¹⁰. In interpreting this mandate, the FAA has created a broad range of internal policies to define, build, acquire, and maintain FAA and contractor operated facilities. In contrast to airborne equipment certification processes, these internal policies are not regulations. They also vary depending upon the type of system capability implemented. This discussion will focus on the process for creating new large-scale capabilities or equipment, or instituting significant changes to the configuration of the NAS.

¹⁰ 49 U.S.C. 40102 Definitions

The FAA uses a set of systems engineering practices and policies to manage the configuration of the NAS. As part of this, the enterprise architecture is a detailed description of operating systems in the NAS, a set of tools for managing the NAS configuration, and as basis for coordinating decision-making for future improvements [74]. When planning new system acquisitions, or changes to existing systems, the FAA employs a set of *configuration management* processes to track and coordinate changes [73]. *Configuration management* is required for any system that is contained in the NAS enterprise architecture [73], which includes most air traffic control communication, navigation, and surveillance systems.

Safety assessment is a defined process within configuration management used to manage the potential risks introduced by changes. Because of its broad uses and impact, the safety assessment process merited a more in depth discussion as a supporting process in Section 3.3. The configuration management process requires a safety review of proposed changes [75]. The depth of analysis of safety differs depending upon the nature of the change.

Results of the safety assessment are documented in a Safety Risk Management Document (SRMD). The SRMD is performed as part of a more general systems-engineering process known as a NAS Change Proposal (NCP). NAS change proposals [73] originate from FAA lines of business and external contractors, and document proposed changes to NAS architecture. Safety decisions are audited by the safety arm of the air traffic organization, ATO-S, and can also be audited by an independent line of business, the office of Air Traffic Oversight (AOV) [11].

When all analysis of a change is complete, the formal review by the appropriate Configuration Control Board is performed to formally approve the proposed change in a NAS Configuration Control Decision (CCD). At this point, safety requirements generated from the safety review have become part of the overall program requirements, which are then approved and implemented through a broader Acquisition Management System (AMS) Process.

The AMS is FAA policy governing the procurement, deployment, and management of FAA products and services [76]. Acquisition processes are structured around a set of decision points by the FAA Joint Resources Council (JRC), the senior investment review board of the FAA. Decisions from the JRC precede review by the White House Office of Management of the

Budget (OMB). Lines of business (such as the Air Traffic Organization) propose and structure programs for review by the JRC and eventual implementation into the NAS [76].

Each milestone in the AMS has a requirement for performance of safety assessment activities to varying levels of fidelity [11]. Safety assessment is one *specialty process* performed to support the AMS [54]. These safety assessment activities vary depending upon which organization initiates the activity and what the nature of the change is. There are also associated programmatic and budgetary review milestones associated with the lifecycle of the change.

3.4.7 Software and Complex Electronic Hardware

The use of software has increased in modern systems, both in airborne avionics and in ground-based systems. This use of software and advanced electronics created a shift from using mechanical methods for providing functionality, to a “virtual” capability to perform similar functions, supported by computer displays and processors. Now, fly-by-wire and glass cockpits are common in aircraft, replacing functionality that was previously performed by mechanical linkages and instrumentation.

This shift from mechanical to electronic functions required new methods for safety assurance. The trend initially spurred the development of DO-178 by RTCA in 1980. DO-178 provides considerations for safety assurance of software in airborne systems. The current revision is DO-178B, which has become a de facto standard for software development in safety critical systems [77].

Software or complex electronic hardware itself is not a component of a vehicle, but is embedded within existing vehicle components, especially avionics. Software also supports functionality in air traffic control systems and displays. Additionally, software-like functionality can be embedded in electronic assemblies, termed “complex electronic hardware. [77]. Because of this distribution in domain, software standards vary for airborne and ground-based software, and for complex electronic hardware. RTCA DO-178B [39] is a consensus standard that was developed as a means of compliance for airborne software certification, and has been applied generally beyond airborne software certification [77]. DO-254 [78] is the airborne counterpart for complex electronic hardware, and is similar in most aspects [77]. Therefore the following discussion will focus on the general process for software. Both documents are recognized by the

FAA through advisory circulars [79, 80] as acceptable means of compliance for assurance of intended function as part of an associated equipment certification.

Design Assurance Levels (DALs) are categories that define the integrity of the software assurance process. The required DAL is determined from the criticality of the function executed by software. This criticality is based on a safety assessment of the potential failure modes of the software, and their associated levels of severity. Guidance on corresponding severity and design assurance level is included in DO-178B [39], FAA systems-level policies, [11], and advisory circulars for aircraft certification [57, 58]. The determination of DAL is based on a safety assessment of the intended function, according to other standards for safety assessment, such as ARP 4761 [31]. Each DAL has an associated set of objectives to be satisfied. Meeting these objectives is required for approval of the software, although alternative means of compliance can be proposed.

Software approval is typically coordinated through an FAA Designated Engineering Representative (DER). The DER is responsible for approving documentation to DO-178B and assisting the applicant in interpreting requirements. Coordination occurs at multiple points in the developmental lifecycle, from initial planning to final implementation and testing. There are multiple formal documents described to coordinate these activities. For more information, see [77].

To interpret the requirements of software approval in ground-based systems, RTCA created DO-278. The document specifies software considerations for approval in use in CNS/ATM systems. It is a companion document to DO-178B, offering corresponding assurance levels and processes to airborne software.

3.5 Other Safety Control Processes

Several additional processes are in place in the air transportation system used to control safety. These processes reside both within the FAA and in other organizations. These processes are not explored in detail, as they are outside of the scope of this work.

3.5.1 Monitoring of Current Operations

Internally, the FAA monitors accident rates and performance of the air traffic control system. Key safety performance metrics serve as management targets for the Air Traffic Organization [81]. Safety trends are also highlighted internally through data analysis efforts such as the Aviation Safety Information Analysis and Sharing Program (ASIAS) [82]. Several other monitoring systems are in place to identify safety issues, typically through voluntary reporting of operators. Examples include the NASA-maintained Aviation Safety Reporting System (ASRS) and the Voluntary Disclosure Reporting Program (VDRP) administered by the FAA.

The National Transportation Safety Board (NTSB) is responsible for investigating major accidents and recommending actions to prevent the future occurrence of accidents. It is separate agency with independent funding from the department of transportation. The role of the NTSB is to issue recommendations based on identified causes of accidents, incidents, or trends identified in the system. The board does not have direct power to implement recommended changes, but has high visibility by the public and Congress.

Several organizations conduct directed studies to identify areas of high risk in the system. Examples include: the NTSB (e.g. Emergency Medical Service Operations [83]), and the AOPA Air Safety Foundation (e.g. the Nall Report [84]), and Congress, through focused hearings. The goal directed studies are to identify accident trends that indicate risk areas in the system that need to be addressed.

3.5.2 Rulemaking

Rulemaking is a general process for agencies of the executive branch to enact new or modified federal regulations. Rulemaking is a general process to perform a set of analysis, modeling, and public comment steps to ensure that there is adequate public visibility of regulations, and that there is adequate need for governmental intervention. Being an executive agency, the FAA is required to follow the rulemaking process for any changes or new additions to the Federal Aviation Regulations [85].

Specific to the FAA, most rules are initially drafted by the agency based on an identified operational need that requires changed to Federal Aviation Regulations. When a major change

to regulations is required, the rulemaking process is lengthy. A GAO study of 76 FAA rule changes found a median time of 2.5 years [86]. The FAA can use Advanced Notice of Proposed Rulemaking to seek input regarding a potential rule, or proceed with a final rule. Industry and stakeholder input is typically obtained through Aviation Rulemaking Advisory Committees formed for each rule. Several analysis tasks before initial implementation of rules assess their environmental impact, cost/benefit distributions, and economic impacts. Analysis prepared by the FAA is coordinated with the White House Office of Management & Budget and Department of Transportation.

3.6 Summary of Safety Assessment for Systems-Level Changes

Proposed changes are approved to two classes of acceptability criteria. The first class is risk-based criteria. In the FAA Safety Risk Management process, these criteria are arranged in a risk matrix. Proposed changes can also be approved to a target level of safety (TLS), which is a threshold risk level for acceptability of a defined event and conditions. The underlying process supporting approval to risk-based criteria requires safety assessment of a proposed change and mitigation of all risks such that all risk levels meet acceptability criteria.

The second class for approval of a proposed systems-level change is performance-based criteria defined in comparison to a reference system. The corresponding approach to designing mitigations will be discussed as the performance-based approach, which can be applied when an acceptably safe example system exists to which the proposed change can be compared.

4 Scoping in Safety Assessment and the Influence Framework

This chapter defines a framework to represent decisions about the appropriate scope of analysis in safety assessment. The scope of analysis is the scope of safety behavior that is examined in detail in evaluation of expected safety performance and is used to reduce complexity of analysis to a tractable level while assessing the most important safety behavior. The framework is applied to three specific approaches to safety assessment analyzed in Chapter 5, detailed analysis of decisions made in assessment of European Reduced Vertical Separation Minima in Chapter 6, analysis of other past changes in Appendix D, and identification of challenges for future changes in Chapter 7.

Based on the investigation of current safety regulatory practices, a general model is presented in the first section that divides safety assessment into sub-processes where common decisions and analysis methods are present. Following this, a framework is developed to describe how scoping decisions should be made, based on the expected influence of components of a proposed change on risk levels.

4.1 Systems-Level Operational Approval Model

A general model of sub-processes within safety assessment was created and is presented in Figure 4-1. The general model is consistent with the FAA's Safety Risk Management (SRM) process as defined in the FAA Air Traffic Organization Safety Management System [11] described in Section 3.3.

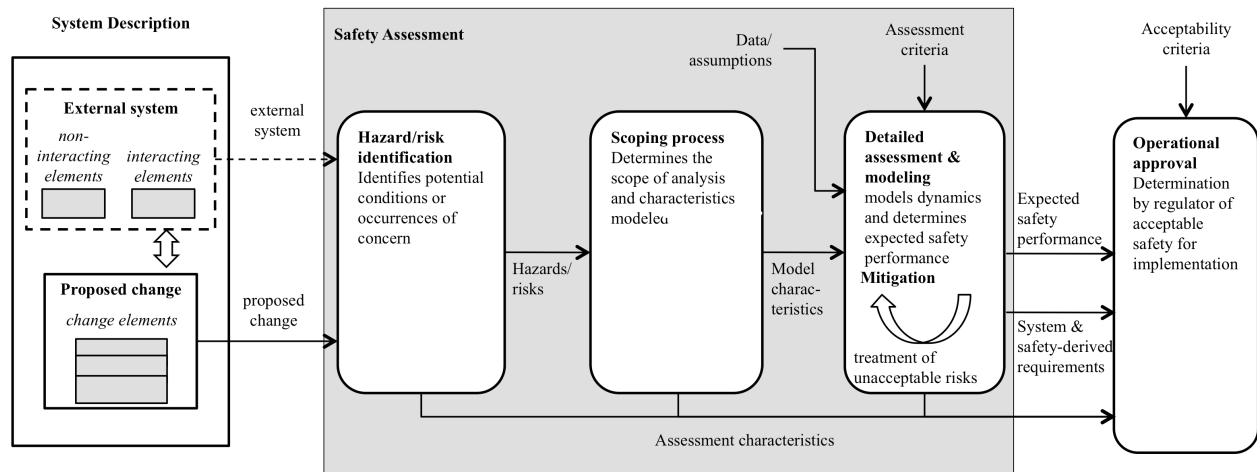


Figure 4-1: Safety Assessment Processes Supporting Operational Approval of a Proposed Change

This general model illustrates the context for the safety assessment process based on a description of a proposed change and the external system to support operational approval. The safety assessment process is shown by the grey-shaded box at the center of the figure. The model also illustrates key sub-processes in safety assessment where decisions are made that influence the safety behavior of a proposed change. These processes include: hazard/risk identification, scoping detailed assessment & modeling, and mitigation. Each sub-process will be described in more detail below.

As shown in Figure 4-1, the input to safety assessment is a description of the proposed change, which consists of change elements and a decomposition of elements in the external system to interacting and non-interacting elements (discussed in more detail in Section 4.2). This system description serves as a basis for hazard/risk identification.

Hazard/Risk identification uses the description of the proposed change to determine potential risks and/or hazards that are associated with the change. The result of this process will be represented by an influence matrix, which is a framework developed in this work. The influence matrix compactly represents the effects of changes in behavior of system elements on associated hazards/risks. The influence matrix is discussed in Section 4.4.2 supported by a conceptual state-based description of safety behavior.

The safety behavior of a real system can be very complex. To better allocate resources to specific areas of concern, safety assessment is typically scoped. The scoping process results in an identification of the scope of detailed analysis, which defines the elements, risks, and conditions that must be included in detailed modeling and assessment. The application of influence matrix to scope is discussed in Section 4.4.

In the process of detailed assessment and modeling, the expected safety performance of the system is evaluated. Data obtained from a variety of sources, such as through operational experience can be used to support the assessment, and assumptions are made in the creation and evaluation of the detailed model. Unacceptable safety performance that does not meet assessment criteria is mitigated through the derivation of safety requirements, and design of additional aspects of the proposed change. The processes of detailed assessment and mitigation are discussed in Section 4.5.

Safety assessment supports an operational approval decision. The output of safety assessment, assumptions and data used, and modeling approaches are also inputs to the operational approval decision. Acceptability criteria are the basis for judging the acceptability of modeled safety performance. They are typically the same as assessment criteria.

4.2 Elements of a Proposed Change

For the systems-level changes, it is useful to divide a proposed change into components, and to describe interactions between the components of the change and components in the external system. These components will be referred to as *system elements*. System elements can be physical (such as avionics, navigation aids, humans, etc.) or virtual (such as procedures or software logic). Properties of system elements may be altered to mitigate unacceptable safety performance.

Types of system elements are further illustrated in Figure 4-2. For a given change, there are elements that are defined by the system boundary of the change. These are typically under design control in the safety assessment process, and are referred to as *change elements*. There are also elements outside of the boundary of the proposed change and part of the external system. Within this category, there are elements with which the change will interact (*interacting elements*). These elements can share physical proximity with the proposed change (e.g. other aircraft operating in the airspace) or have linked and dependent functionality (e.g. GPS satellite signals that are used as a position source). There are also external elements with which the proposed change is reasonably expected to not interact, termed *non-interacting elements*.

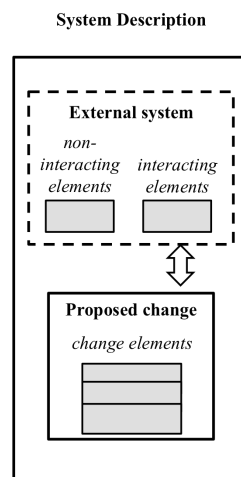


Figure 4-2: System Elements

One way that a proposed change can be described is by a concept of operations, which includes change elements that will be implemented and how the proposed change will operate in the external air transportation system. Another common way is to refer to the description of a proposed change in an Operational Service and Environment Definition (OSED) document.

A proposed change can add new elements to the existing system. This is the case when new physical elements are defined or new procedures are performed in the proposed change. Elements can also replace those currently performing the same or a similar function, in which case the change element is a replacement or modification to an existing element.

Elements of a proposed change enable a set of operational *capabilities*. Capabilities are divided into three areas: airborne capabilities, which include functions performed by aircraft and flight crews; infrastructure-based capabilities, which include ground-based infrastructure, satellite-based infrastructure, or ATC automation and surveillance systems; and procedural capabilities, which include airspace procedures used by air traffic control, operational procedures implemented on aircraft, and airspace design. With the increased use of the Global Positioning System (GPS) as a position source, satellite-based systems have also become part of the NAS navigational infrastructure, and can be considered as similar to ground-based infrastructure and grouped as that capability. These divisions are illustrated in Figure 4-3 with examples of elements within each capability.

Historically, airborne, airspace, and infrastructure capabilities have followed separate and independent assessment and operational approval processes. The current operational approval process reflects this division in approval authority of ground-based, airborne, and procedural changes, as discussed in Chapter 3. However, as proposed changes have become more distributed, there is increased coordination across approval processes in identifying common safety requirements early in the development of new systems capabilities [36].

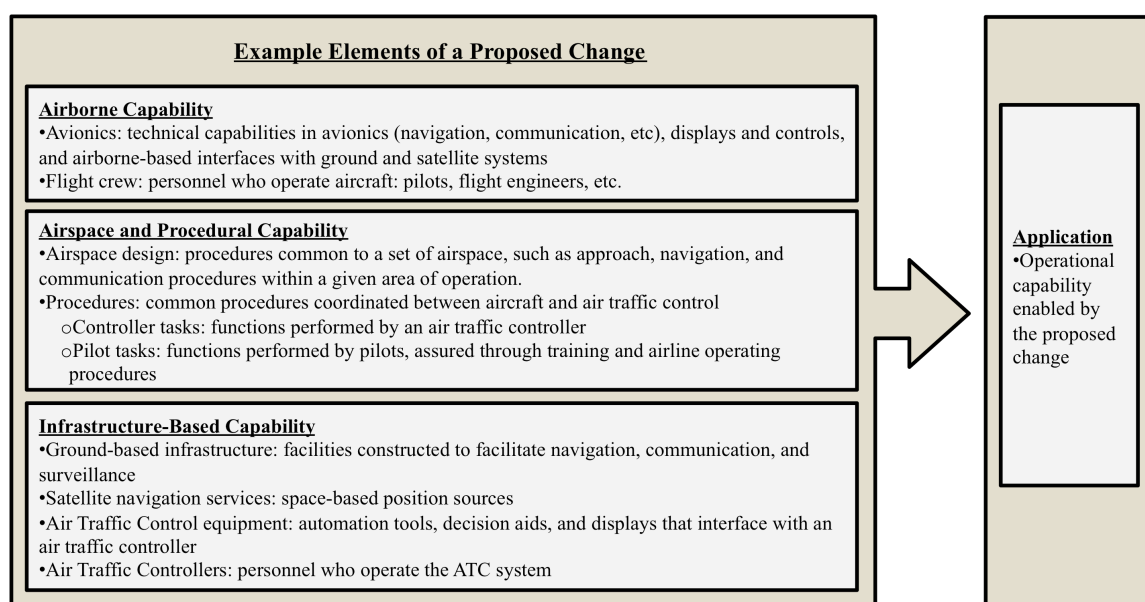


Figure 4-3: Elements of a Proposed System and Enabled Applications

Individual capabilities combine to enable an *application*, as illustrated in Figure 4-3. The application describes the function enabled by the proposed change. Elements of a change are can vary depending upon the application performed by that change.

4.3 The Influence of System Elements on Safety

4.3.1 Abstractions Used in Safety Assessment

Safety assessment supporting current operational approval processes relies on estimating the level of risk associated with a proposed change. To support the analysis of safety assessment decisions, it is therefore useful to provide further definition of how system elements affect risk levels. One approach to representing the relation of safety behavior to risks is based on a state - representation, illustrated conceptually in Figure 4-4. In this representation, a circle represents each state of a system, which is a defined set of conditions under which the system is operating. Transitions between states are depicted as directed arcs. Transitions are the result of occurrence of events. When multiple arcs reach a state, the state has multiple predecessors, any one of which could lead to that state. These events could be failures, changes in the environment, or the effect of other components of the system. Transitions can be assigned a probability or rate, allowing state chains to be evaluated stochastically.

Initiating states are defined as *causes*, often called root causes. Intermediate states can be contributing causes. The set of final states are risk events. The conditions in a given state a result of the events predicted to lead to the state. These conditions can describe several aspects of the state. They can indicate that the system is operating in a failed mode, such that a failure preceded entry into the state. They can also indicate the associated state of the operational environment, such as being on final approach, or operating in a thunderstorm.

The relationship of causes to risks is the *safety behavior* of the system. In Figure 4-4, safety behavior is illustrated for an individual risk. The behavior leading to risks is often a complex combination of multiple causes and states of the environment. In the course of assessment, risks also may not be the only outcomes evaluated. Causal chains can terminate in outcomes without associated harm. For simplicity, the behavior shown in Figure 4-4 does not reflect this full complexity. Risks are assigned levels of severity based on the harm associated with them. Examples of levels of severity assigned to risks were discussed in Section 3.3.

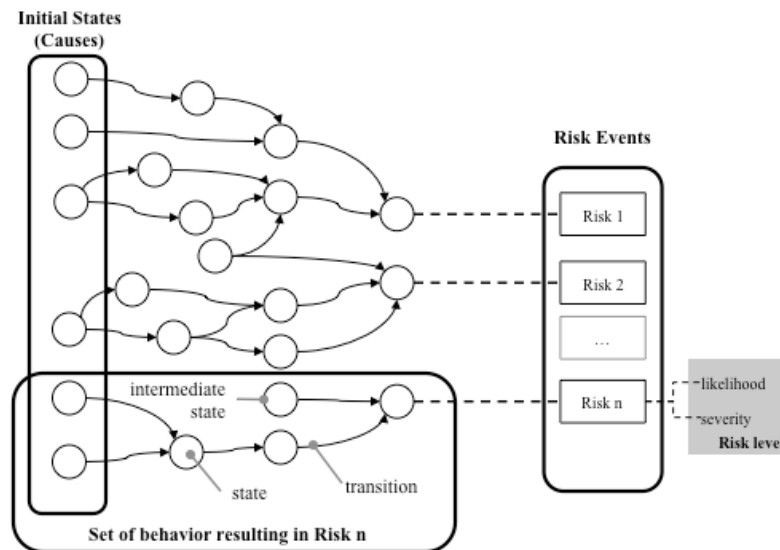


Figure 4-4: State Transition Representation of Safety Behavior

Safety behavior can also be understood through the intermediate abstraction of a hazard, defined previously in Chapter 2 as a set of conditions in the system that could result in harm. In the state-based representation, the state defined by this set of conditions is referred to as the hazard. The intermediate nature of a hazard is illustrated by an abstract example in Figure 4-5, which can be contrasted with Figure 4-4. In this example, the states between causes and risks have been grouped into three hazards, indicated by the dashed boxes. Hazards have an associated likelihood, but do not directly have an associated severity measure, as they are not occurrences. An intermediate state can only be classified as a hazard if it leads to a risk event.

A hazard is used in safety assessment for several reasons. As an intermediate state, it allows both forward and backward search to be used to define states of concern. Forward search is the process of identifying initial states, and then considering potential hazardous states that result from the initial states. Backward search is the process of considering risks of concern, and identifying conditions under which the risks can occur. Each strategy is likely to identify a broader set of safety concerns than an identification of hazards alone [87].

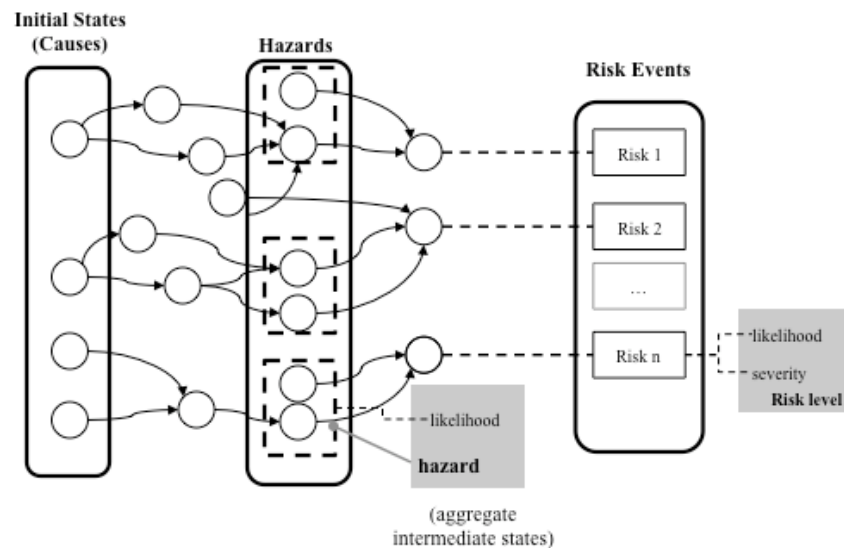


Figure 4-5: A Hazard as an Intermediate State

Because of its nature as an intermediate state in a chain of events leading to risks, the definition of a hazard can vary in its level of abstraction. A hazard can be abstracted closer to preceding events, which is common in failure-based definitions of hazards. It can also be defined closer to risks, where it can be a general category of harm, such as a midair collision. This level of abstraction would depend on where the hazard box placed in Figure 4-5, either to the left (toward causes) or to the right (toward risks).

A common view of causal states, hazards, and potential outcomes is the bow tie model, shown in Figure 4-6 for the behavior surrounding a single hazard. This model views hazards and outcomes differently from the direct causal chain of Figure 4-4. It is a combination of state and event-based abstractions. Root causes are shown on the left side of the model as initiating states. Safety behavior is evaluated through contributory causes to a hazard. The behavior evaluated can be complex, through several intermediate states and conditions.

From a hazard, the representation of behavior shifts to an event tree. Succeeding events are modeled as branches of the tree, where the potential states of a system have multiple, discrete paths to risk events. The event tree notation is valuable, as it illustrates event transitions that are commonly related to all occurrences of a hazard as branch points.

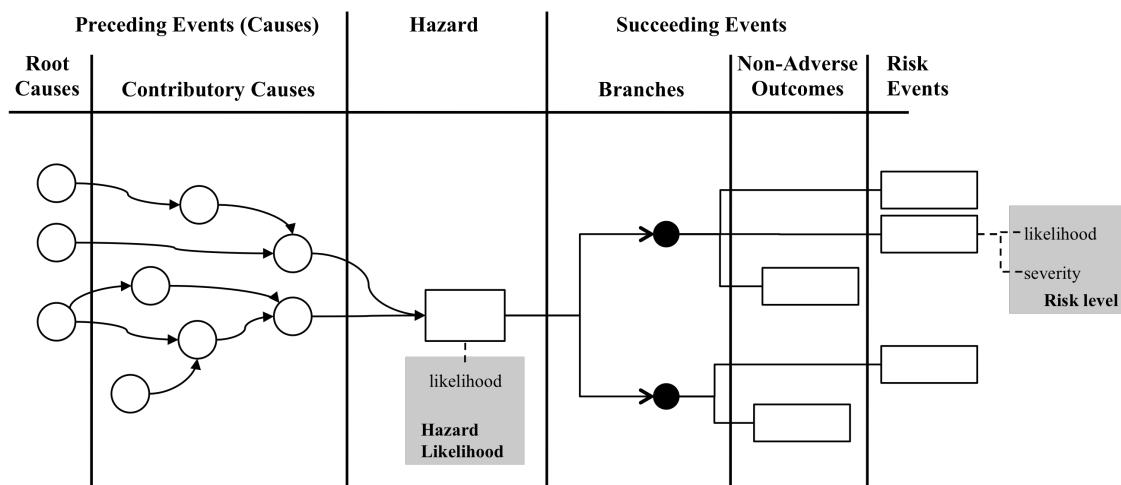


Figure 4-6: Hybrid Bow-Tie Framework of Hazard Analysis

The addition of the event tree representation makes succeeding events more distinct. States preceding the hazard can often have complex relationships. These are commonly represented in the bow tie model by a fault tree [11]. Fault Tree Analysis allows the complex causal relationships to be captured using logic-based combinations of events and associated probabilities [88]. To make the severity associated with final event tree states clearer, a distinction between final risk events and non-adverse outcomes is made in Figure 4-6.

Other processes can be used to evaluate risk, including Operational Safety Assessment (OSA) and Operational Performance Analysis (OPA) that consider safety behavior based on operational scenarios. Safety behavior can also be evaluated through risk models, as is the case in Collision Risk Modeling (CRM).

The complex relationship of events and conditions leading up to the hazard result in a measure of likelihood associated with the hazard. Based on the behavior of the system following the hazard, there is also a likelihood associated with each outcome. For risks, this likelihood is the risk level.

Because real systems exhibit complex dynamics, multiple hazards may lead to multiple risks. This is shown notionally in Figure 4-7. For example, it can be noted that both *Hazard 1* and *Hazard 2* influence Risk 3. When there are multiple hazards that influence the level of given risk, the total level of risk is the result safety behavior through all associated hazards.

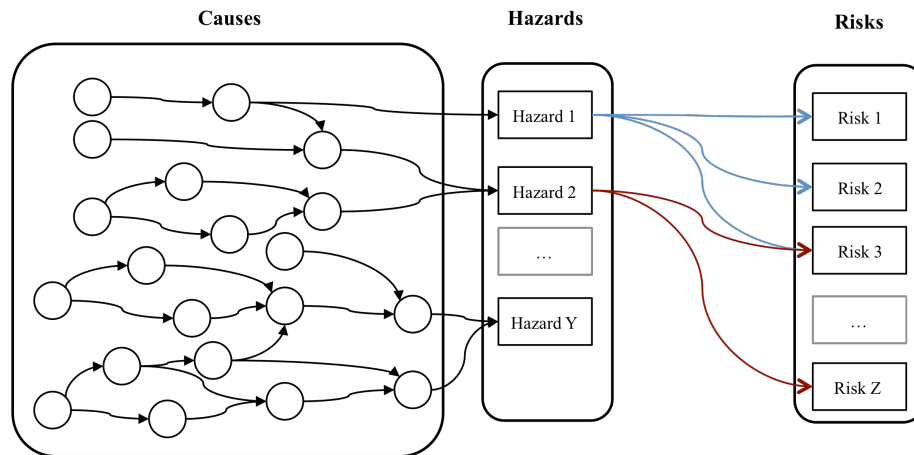


Figure 4-7: System Behavior with Multiple Hazards and Risk Events

4.3.2 Scoping in Safety Assessment

The large scope of potential safety behavior in real systems can be intractable to completely analyze. There can be a near-infinite combination of conditions in the system, potential behavior of system elements, and associated risks. There is therefore, a practical need to limit the safety behavior evaluated, to make analysis tractable and more efficient. Limiting the safety behavior evaluated in a proposed change is defined as setting the *scope* of the safety assessment.

The scoping process represents a decision made by safety assessors that defines the required characteristics of a model of a proposed change. Scoping decisions can have strong implications on the safety of the system when implemented. Inappropriately defining scope can lead to unexamined behavior that increases the level of risk in operation. Defining scope as too large can lead to overspecification, where mitigations are applied that were not necessary. Overspecification can have the effect of increasing the expenditure of resources in the system that could be more efficiently applied to other safety concerns.

There are three factors that define the scope of analysis. The first factor is the breadth of elements of a system that are evaluated. The second factor is the depth of risks that are examined. This is the number of adverse events that are analyzed and/or quantified. Behavior of elements and risks can also be evaluated for several conditions, the third factor of scope. Conditions are scenarios or assumptions describing the operational state of the system, such as states of the environment, flight phases, etc. Conditions are not system elements, as they do not have behavior that can be modified to influence the level of risk. Safety can also be assessed for

an average condition, which might represent several different potential scenarios or operations aggregated into an average level of risk.

Hazards define the set of conditions that can potentially lead to risks, while risks are events associated with harm to people and property. Individual risks can occur following multiple hazards or, conversely, individual hazards may lead to multiple risks, as illustrated above in Figure 4-7. Because hazards and risks are linked in sequence, they can be defined as related dimensions of scope. This is illustrated in Figure 4-8. When viewed in terms of risk, the scope implicitly includes all hazards that contribute to the risk. When defined by hazards, all risks associated with the hazard are within scope.

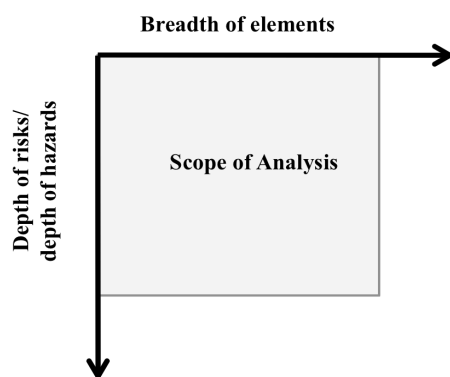


Figure 4-8: Dimensions of Scope: Elements, Hazards, and Risks

4.3.3 Changes in Safety Behavior due to Changes of Elements and Influence

Implementing a proposed change will change safety behavior and associated levels of risk in the air transportation system. This change in behavior can be decomposed by the effect of system elements. By this view, a change in an element's behavior can influence hazards and risks through several mechanisms, illustrated through the hybrid bow tie model of Figure 4-6. This is shown below in Figure 4-9, where the influence of changes in elements on safety behavior has been highlighted. Figure 4-9 shows a bow tie model for one hazard for clarity. However, the influence of system elements on multiple hazards and risks in a real system would be illustrated through multiple bow tie models.

There are two sets of events shown in the bow tie model. On the left-hand side, preceding events occur before a hazard and influence the likelihood of the hazard. Changes in behavior of system

elements can influence the likelihood of hazards, by affecting the probability of occurrence of the contributory causes shown on the left-hand side. This is shown by shaded states on the left-hand side of the figure, and a shaded transition path.

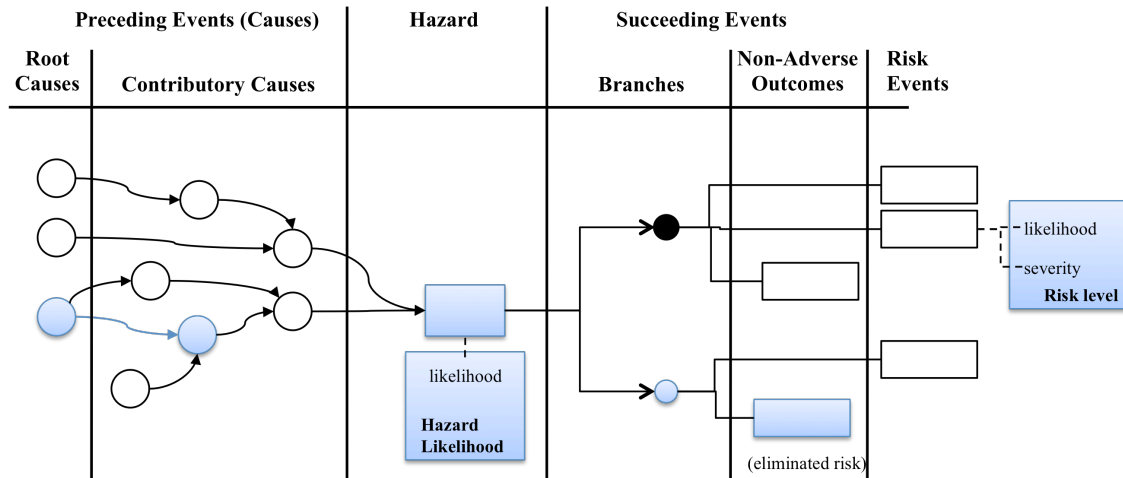


Figure 4-9: Influence on Safety Behavior of a Proposed Change in the Bow Tie Model

The second part of the bow tie model is an event tree of events succeeding a hazard. Changes in behavior of system elements can also influence the likelihood and structure of these succeeding events. In some cases, system elements can add a mitigation that results in the elimination of risks. This creates a branch in the event tree with a high likelihood of a non-adverse outcome, as shown by the eliminated risk as the bottom event in Figure 4-9.

To understand scoping decisions, it is useful to define a characteristic of the relationship between system elements and risks on which scope decisions are based. For this reason, influence is defined conceptually in Figure 4-10. *Influence* is a measure of the change in risk level of a given risk (R_i) due to a change made to a system element (E_j). Influence of a given element and risk level is evaluated through expected safety behavior of the system. The determination of influence is normally based on the judgment of a safety assessor. It should also be noted that a change in a system element could also change the severity associated with a risk. This dynamic is not captured in the framework and would require further refinement in future applications of influence.

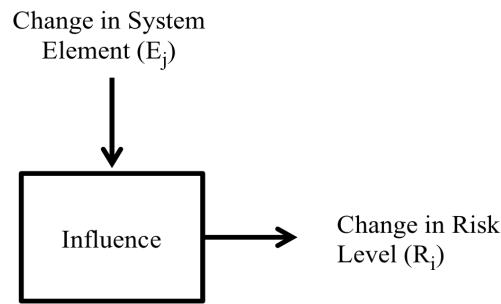


Figure 4-10: Influence Defined

The change in a system element is defined around a design point, which is usually the state of the element from the initial system description. It is not a change in behavior from the existing system. By this definition, influence represents the ability to affect a level of risk based on design decisions to set specific properties of a system element.

System elements can be an aspect of the system for which an explicit parameter is related to safety performance. An example would be navigation precision. By some collision risk models, risk is defined mathematically as a function of aircraft navigation performance. System elements can also be aspects of the system without explicit parameters relating it to risk. An example of this type of system element is flight crew training. While training clearly influences some risks, it may not be parameterized. To capture both of these types of elements within the influence framework, the function is defined conceptually and represents the effect of a change in behavior of an element on risk levels. These changes do not necessarily have to be continuous or parametric.

Influence as defined here also does not have a positive or negative sense. Influence may represent that changes to a system element can expected to only increase risk level, only reduce risk level, or increase or reduce risk level depending upon the properties of the element. Influence will be coded based on its absolute magnitude, as described in the following section.

In a proposed change, there are typically multiple system elements and risks affected by the change. Multiple measures of influence will be arranged in this work in the form of an $m \times n$ *influence matrix*, an illustration of which is shown in Figure 4-11. The columns of the matrix denote system elements (E_j), and the rows of the matrix denote risk events (R_j). Each cell of the matrix is the influence of the corresponding element and risk.

The influence matrix presents a method of analyzing how scoping decisions should be made. The influence matrix framework will also be used to depict how decisions have been made in past changes and to illustrate the implications of current safety assessment approaches.

The influence matrix representation assumes a linear decomposition between elements and risk. Each influence value is constructed independently of other system elements. Although this is a limitation of the framework, it does not imply that expected safety performance of a system is the result of a linear combination of the safety performance of individual elements. As a system is typically decomposed when scope decisions are made, the influence matrix representation is appropriate for describing scope decisions. Interactions between elements will exist in a real system. The complexity in interaction is captured in the detailed modeling and assessment process, when expected safety performance is evaluated in detail.

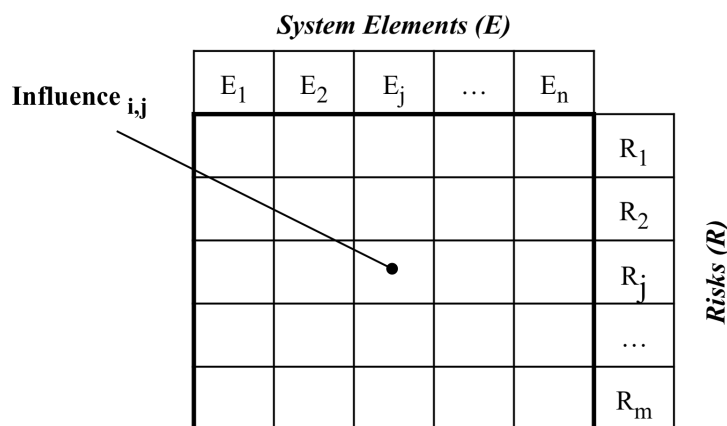


Figure 4-11: Influence Matrix

Because of the linear decomposition of the influence matrix, there are limitations in identifying correlated or dependent risks. Dependent risks can result from the behavior of a combination of elements acting together. When examining the influence of any given individual element, this correlation may be captured if it is recognized by the assessor, as the behavior of that element changes as a result of the correlation and has an influence on risk. However, the influence of combinations of elements is more likely to be overlooked through this process, and this is a limitation.

4.4 Application of the Influence Matrix to Scope Decisions

Scoping decisions can and their implications can be represented through the influence framework defined above. In this section, the method of creating an influence matrix for a proposed change will be described with a notional example.

4.4.1 Creation of Influence Matrix for a Proposed Change

Before the scoping process, risks or hazards associated with a proposed change must be identified. To construct an influence matrix, it is necessary to examine what behavior contributes to each risk, and the strength of influence of that behavior. To illustrate this process, a notional set of influences on a single risk is shown in Figure 4-12.

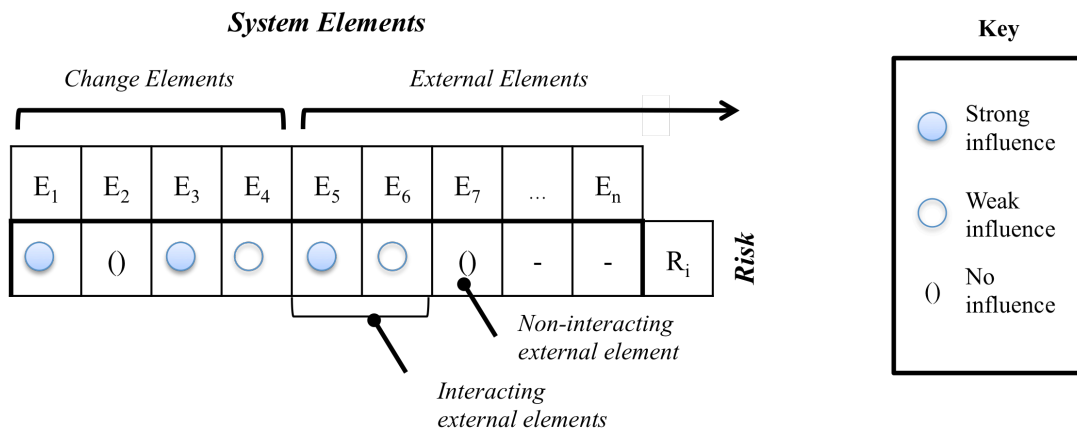


Figure 4-12: Notional Influence of System Elements on a Single Risk

The construction of an influence matrix follows the process of defining influence for each risk. It is a subjective process that can be applied by safety assessors to capture judgment regarding key factors affecting the scope of assessment. Throughout this work, the magnitude of influence will be coded by three categories. A filled circle indicates a strong influence. If a given influence is strong, changes in behavior of the element can result in a large change in the associated risk. An empty circle indicates weak influence. When influence is weak, changes to behavior impact the associated risk, but at a lower level of magnitude. Weak influences can often act indirectly or in combination with other elements in the system. Closed parentheses indicate no influence. In this case, there is no relationship between the system element and associated risk. Changes to the system element do not change the magnitude of the risk.

In Figure 4-12, the notional influence of change elements and external elements for a given risk, R_i , is shown. Four change elements (E_1 - E_4) constitute the proposed change. For a real change, this set can be large or small depending upon how analysis is parsed. There are three external elements (E_5 - E_7) shown with assigned influence. The additional elements in the system (up to E_n) do not have evaluated influence, as indicated by the dashes. They are shown to illustrate that the set of external elements can be expansive, encompassing all elements of the air transportation system.

Elements have been assigned notional influence rankings in Figure 4-12. For the change elements, it should be recognized that some elements of a change (e.g. E_7) would not have an influence on risk.

When external elements have an influence on risk, it is due to that interaction with change elements. This interaction is often referred to as coupling [25]. Elements in the external system are generally outside of the authority of the system designer. Therefore, their magnitude of influence does not represent a level of risk control achievable through that system element. Instead, influence is a measure of the strength of interaction due to the properties of a change element. When considering the influence of external elements, the change elements are evaluated and controlled to achieve acceptable risk levels in the presence of external interactions.

As an example, E_5 has been assigned a strong influence on risk. This would indicate that the behavior of that element could significantly alter the risk level depending upon how the proposed change interacts with it. Its contribution to the level of risk varies based on the configuration and detailed properties specified for the change.

In cases where justification is provided for assessment of risk levels, influence is discussed in safety assessment documentation. It is asserted by the assessors that behavior of a given element affects the level of risk under investigation. In other cases, the presence of influence is captured implicitly by the inclusion of elements in structured models, such as fault trees or event trees. This does not, however, explicitly capture the strength of influence.

4.4.2 Influence Matrix and Scope of Analysis

It is a challenge to determine the appropriate scope of analysis. The scope of analysis is required to limit complexity of the assessment task; therefore it should not include risks or system elements for which implemented behavior will meet acceptability criteria without modification. However, it must capture all potentially significant influences on risk above some acceptability level, which is difficult to achieve before the true risk levels are known. There can also be multiple separate analyses conducted in safety assessment. If this is the case, there can also be multiple scopes of analysis identified.

Several strategies can be used to determine the appropriate level of scope, and the influence matrix will be used here to illustrate those strategies. To illustrate scoping decisions with the influence matrix, a notional influence matrix for a proposed change is shown in Figure 4-13. Similar to the example above, there are four change elements, but only two external elements shown with influence. The additional external elements are assigned no influence. There are eight risks shown with assigned influence. The risks have been grouped by two categories of severity (catastrophic and hazardous). The scope of assessment is shaded in grey and bounded by a rounded box.

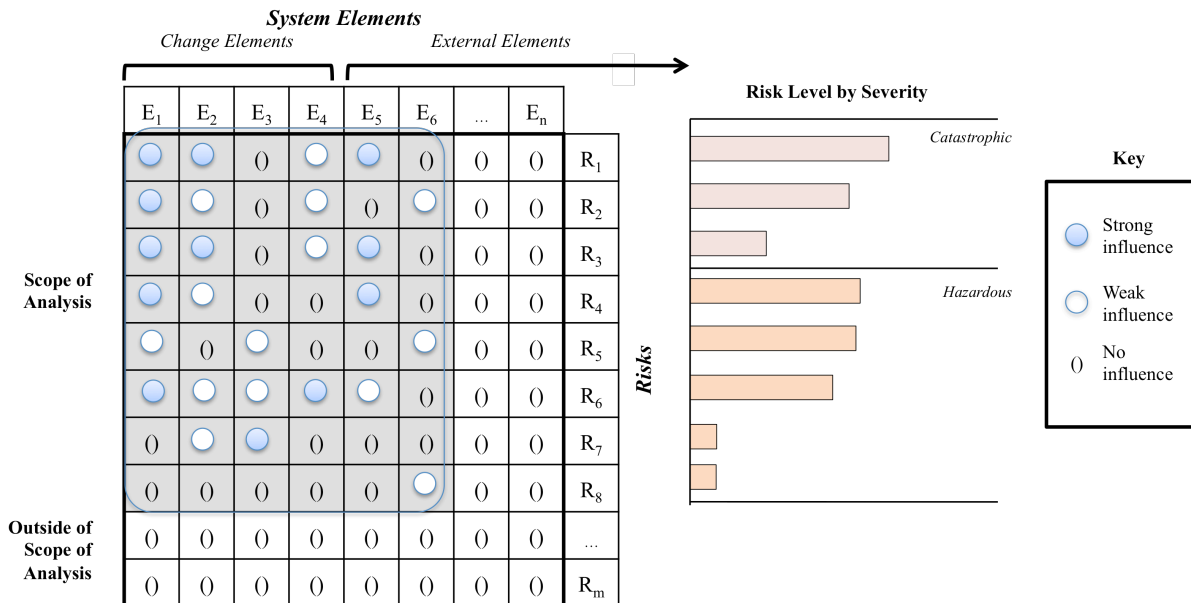


Figure 4-13: Notional Influence Matrix and Level of Risk for a Proposed Change

Notional risk levels are shown in Figure 4-13 assigned to each risk. These represent a judgment of the risk level made by the assessor when hazards and risks are identified. Risk level will be an important factor in eliminating some risks from scope, as described in the following sections.

It should be noted that influence defines the effect of a change in an element on change in level of risk. The amount that the risk level can be altered in the design of mitigations is related to, but distinct from the aggregate influence of system elements on the risk. There can be risk events with very low levels of risk and strong influence, as shown for Risk 7 and Element 3 (R_7 and E_3) in Figure 4-13. Changes to E_3 may strongly correlate with the level of R_7 , but the overall magnitude of the change in level of risk can be insignificant compared to other risks.

Up to this point, the influence matrix has been arranged by risk. The processes of safety assessment and scoping can also be performed using hazards, with acceptability criteria expressed for risk levels by hazard. The inclusion of this process in the influence framework bears more detailed discussion.

Because hazards are an intermediate state between initial causes and risks, a given risk can be influenced through multiple hazards. An example of this is shown in Figure 4-14. There are three hazards and five risk events that follow the hazards. Two levels of severity are also shown in the example. Each hazard precedes two risks, which would be represented by an event tree with one branching point. Risk 1 is influenced by two hazards: Hazard 1 and Hazard 3. Risk 2 is only influenced through Hazard 2, Risk 3 only through Hazard 1, and so on.

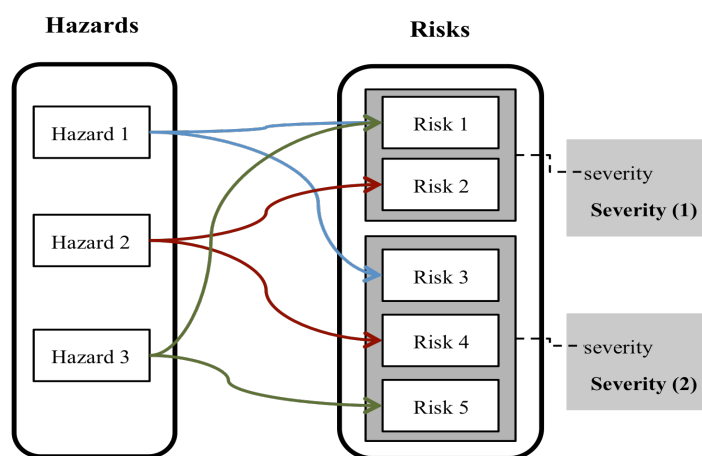


Figure 4-14: Example of Hazard Mapping to Risks

In the example above, if influence is decomposed by hazard, there are two sets of influences of Risk 1 (R_1). The first set is a representation of safety behavior that results in Hazard 1 (H_1), and then results in Risk 1. The second set is a representation of safety behavior that results in Hazard 3 (H_3), and then results in Risk 1. These influences can be very different than aggregated safety behavior that results in Risk 1. As shown in Figure 4-15, separating by hazard, shown in the right side, disaggregates the influence of elements through hazards. This is common in hazard-based safety assessment approaches, and its implications on scope will be discussed in the following chapter.

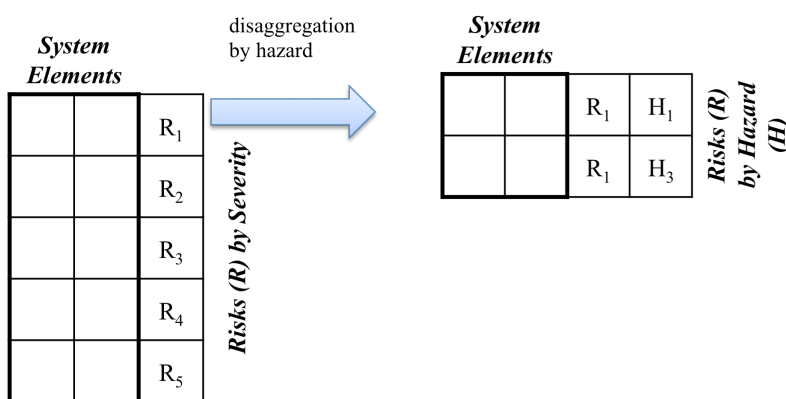


Figure 4-15: Arrangement of Influence by Hazard vs. Risk

4.4.3 Elimination of Risks from Scope

There are several general scoping strategies that are applied across multiple safety assessment approaches that will be discussed below.

Scoping by Dominant Risk. As described in Section 4.4.2, there can be an initial level of risk judged by the assessor during hazard identification. Based on this level, other risks may be scoped out by dominance. Scoping by dominance is appropriate when there is similar safety behavior of elements within the scope of analysis. This results in a similar structure of the influence matrix across risks. It is assumed that the similar structure of influence will lead to similar mitigation effectiveness across all risks. If this is the case, then the dominant risk is that with the highest level of risk and must have a higher or equal severity level than other risks. If this risk is mitigated to an acceptable level, then all other risks will be at acceptable levels. The

lower magnitude risks are therefore scoped out of detailed analysis, as they are dominated by the higher risk.

Scoping by dominance is illustrated in Figure 4-16. The six elements shown have similar strength of influence across the four risks shown. The risk level and severity of each risk are also shown. Risk 1 has the highest level of risk and is the highest severity risk. Therefore it dominates and other risks can be eliminated from the scope of analysis. Although the strength of influence is similar across risks, this is not sufficient to assert that behavior is similar. The identification of similar behavior is not shown in the influence matrix, as noted below the matrix.

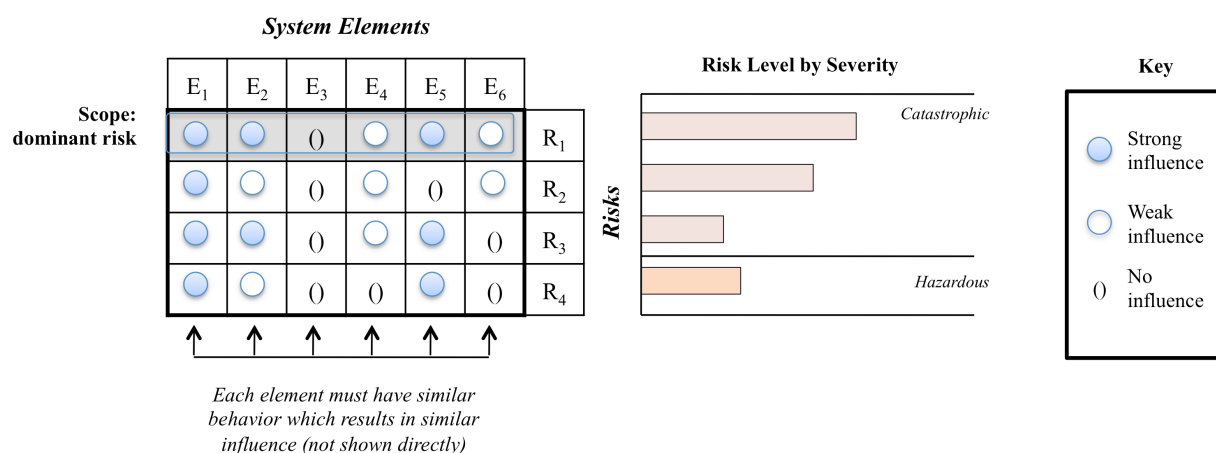


Figure 4-16: Scoping by Dominant Risk

The use of scoping by dominance is typically applied when organizing safety assessments by hazard. As described previously, there are several risk events that can follow a hazard, depending upon succeeding states. Instead of evaluating the acceptability of all risk events, risks are pruned to consider the dominant risk associated with each hazard in the analysis.

An additional method for scoping by dominant risk is by analyzing risk levels under a worst-case operating condition or state of the environment. Hazards are defined by a set of conditions. These conditions can be an operating state of system, such as a flight condition, or assumed load on the system (e.g. traffic density, communication rate, etc). It can also be an environmental condition, such as visibility (e.g. IMC or VMC), weather, or turbulence. Scoping by this method functions similarly to the example shown above in Figure 4-16, but may not necessitate the judgment of associated risk levels. Instead, it is assumed that the worst expected operation

conditions will have the highest level of risk, and the risk level of other conditions will be adequately mitigated. It should be noted that it might not always be possible to determine the worst case operating condition expected in the operation of a system.

Scoping Negligible Risks. In some cases, risks are eliminated from the scope of analysis if they can be considered to be negligible. Negligible risks are those for which the initially assessed risk level is lower (and usually substantially lower) than acceptability criteria. Influence of elements on negligible risks must also be weak. This reduces uncertainty that the risk level will be made unacceptable by mitigations applied that change the behavior of system elements. The combination of weak influence and low level of risk indicates that over any potential range of behavior, risk is not expected to change substantially. If influence is strong, however, it may not be appropriate to eliminate negligible risks from scope, as their risk level may increase depending upon the specific behavior assessed in the detailed analysis and modeling.

Scoping Uncontrollable Risks. There are some risks that are fundamentally not controllable. For uncontrollable risks, there is no influence across any system element. Thus, the risk level cannot be changed regardless of any mitigation that may be applied to the risk. An example of an uncontrollable risk is a meteor strike. A potential loss of life due to a meteor impact with the earth exists for any proposed change. However, its causes are not within control of the air transportation system. Because of this, resources are typically not devoted to assessing its level of risk or modeling its effects.

Scoping by the Change Boundary. There are likely to be risks present in the system that exist, but are not influenced by the behavior of the proposed change. These are appropriate to eliminate, as it is not possible to mitigate them through requirements placed on the proposed change.

Scoping Through Similarity. Risks can be scoped out of analysis through similarity. Similarity is the degree to which the safety behavior related to a given risk or set of risks is expected to be the same as that of the current system. If the current system is accepted as safe, then the behavior in the proposed change can be accepted as safe without fully analyzing the level of risk for a subset of risks associated with the change. This assumes that the behavior after implementing the change is sufficiently similar to the existing behavior that it will be acceptable.

Figure 4-17 illustrates the use of similarity to scope risks. In the example, Risks 1-3 (R_1 - R_3) are within the scope of analysis and influence is assessed. Risks 4-5 (R_4 - R_5) in the example are scoped out by similarity. Influence is not directly evaluated, and the risks are eliminated from scope as their risk level is expected to be similar to an existing, acceptable system.

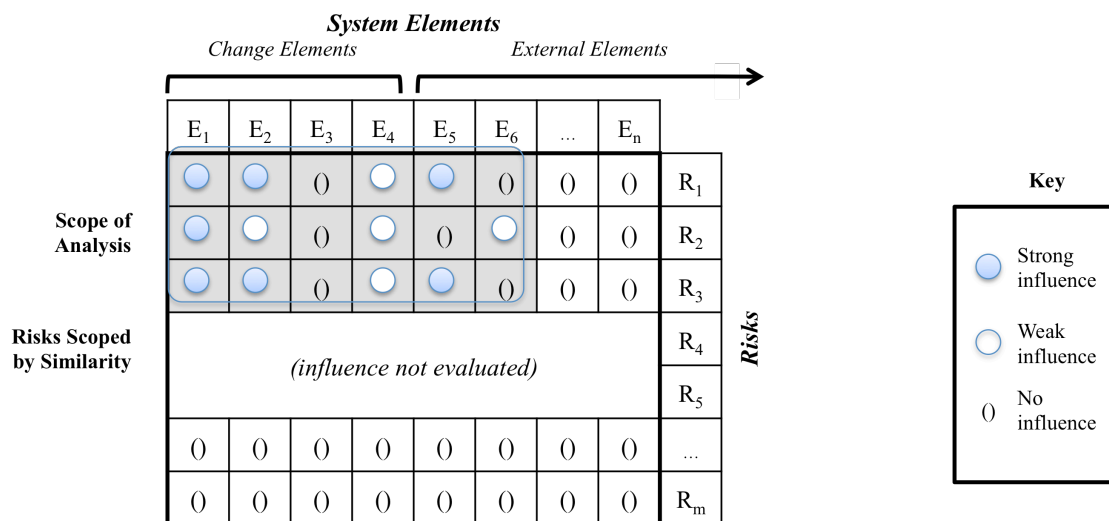


Figure 4-17: Use of Similarity to Scope Hazards Assessed

4.4.4 Unknown Risks and Scope

There are likely to be unknown risks present in the assessment of a proposed change. Unknown risks can arise from safety behavior or conditions that were not conceived in the hazard/risk identification process. They can also result from unknown and unpredictable interactions with the external system. Emergent behavior is one class of unknown risks, which is behavior that was not predicted at the level of abstraction at which the system was viewed. Unknown risks are shown conceptually in the influence matrix framework as entries with unknown influence across all system elements, illustrated in Figure 4-18.

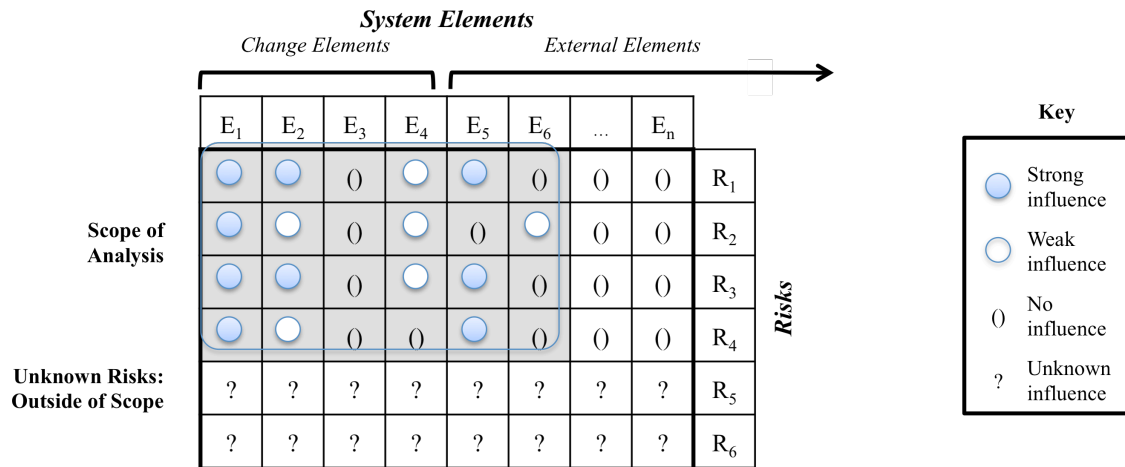


Figure 4-18: Out of Scope Unknown Risks

4.5 Detailed Assessment and Modeling/ Mitigation

From the scoping process, required characteristics for detailed assessment and modeling/mitigation are derived. These characteristics serve as the set of behavior that should be evaluated in more complex models. This is illustrated using a feedback representation in Figure 4-19. Model characteristics serve as an input to the detailed assessment & modeling process. The result of the process is the expected safety performance of the proposed change. This performance is compared against assessment criteria to determine unacceptable safety performance that must be mitigated. Mitigations are then determined and implemented as safety-derived requirements through properties of system elements, or additional system elements. When all expected performance meets assessment criteria, the change is proposed for operational approval.

A proposed change is normally assessed to the same criteria as used in judging acceptability for operational approval. This ensures that the assessed behavior of the system will be sufficient to ensure acceptability when implemented.

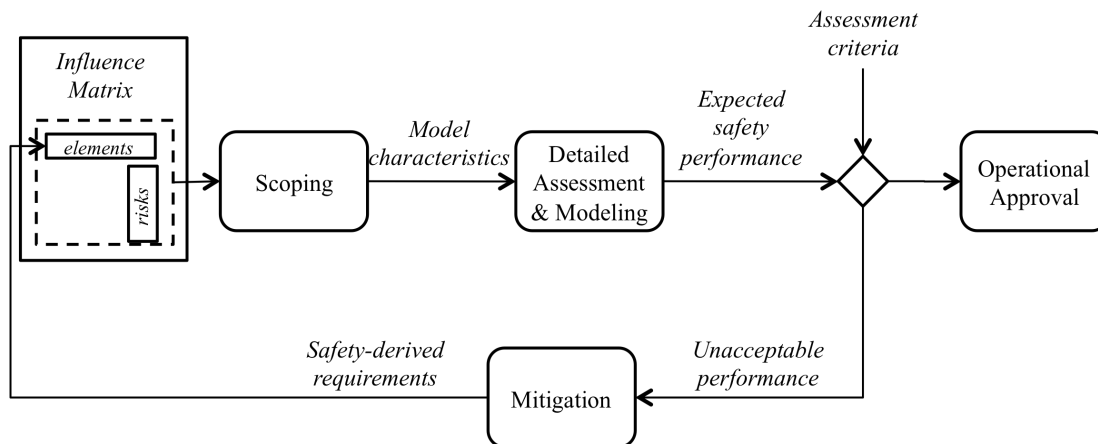


Figure 4-19: Safety Assessment and Safety-Derived Requirements

The approach for performing detailed modeling and assessment varies depending upon the assessment criteria. Different approaches are described in more detail, along with each associated criterion, in Chapter 5.

4.6 Operational Approval

Operational approval by a regulatory authority is necessary before implementation of a systems-level change. Operational approval can depend upon combinations of decomposed approval decisions for separate components, as discussed in Section 3.2. In this work, operational approval is focused on the approval of the expected safety performance of a proposed change.

As introduced in Figure 4-1, and reprinted here as Figure 4-20, there are multiple inputs to the operational approval process. One input is expected safety performance. This performance typically must meet safety acceptability criteria that serve as a basis for the operational approval decision. In some exceptional cases, approval may be granted for changes that do not meet acceptability criteria. In addition to expected safety performance, the system and safety-derived requirements are also considered in the operational approval process.

It is important to note that human regulators conduct operational approval. Therefore, it is typically not sufficient for the modeled safety to simply meet acceptability criteria. As part of the operational approval process, several characteristics of the safety assessment are also considered. The scope decisions, choice of model, and assumptions made in detailed modeling

must have the confidence of the regulator. If there are sufficient uncertainties or unsupported assumptions, this may result in approval being denied.

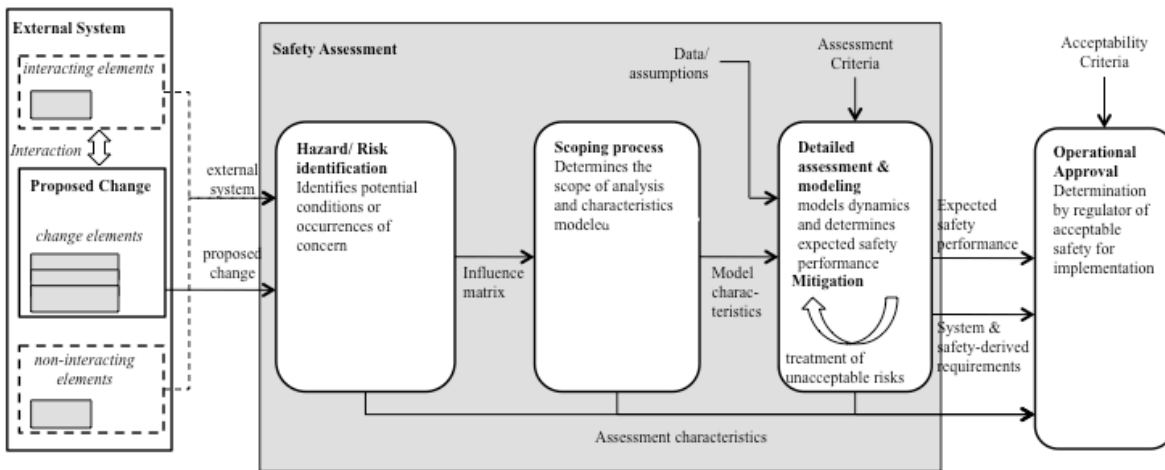


Figure 4-20: Safety Assessment Processes Supporting Operational Approval of a Proposed Change

Involving regulatory representatives in the safety assessment process is typically used to mitigate the risk of approval rejection. This ensures that appropriate decisions are made regarding analysis scope and detailed assessment methods. It can also serve to familiarize regulators with the proposed change, and any embedded assumptions made.

5 Analysis of Safety Assessment Approaches Using the Influence Framework

Based on the investigation of current safety regulatory practices, there are two classes of acceptability criteria used in safety assessment of proposed systems-level changes: risk-based criteria and performance criteria. Within the class of risk-based criteria, there are two types: a risk matrix and a Target Level of Safety (TLS). For each criterion, there is a distinct approach to conducting safety assessment with different processes for hazard/risk identification, scoping, and detailed modeling and assessment. This chapter will describe these key differences utilizing the influence framework developed in the previous chapter.

The risk matrix approach is discussed first, following by the TLS approach. The performance-based approach is discussed in the third section. Each subsection of the approach begins with a description of the approach and criteria and is then organized by the general process divisions in safety assessment: hazard/risk identification, scoping, detailed modeling and analysis, and mitigation.

5.1 Risk Matrix Approach

A risk matrix is a risk-based criterion that defines a risk ranking of an event based on two factors, each forming a dimension of the matrix. The first factor is the severity of the risk. Severity is defined based on descriptions of harm associated with a risk or example events that fit the category. The second factor in a risk ranking is the likelihood of a risk, referred to in this work as the risk level. Each likelihood category has associated qualitative and quantitative definitions. Definitions of severity include measures of the occurrence of harm to people and property and indicators of harm. The implications of this will be discussed at the end of section 5.1.2 (For examples of severity definitions, the reader may refer to Section 3.3). The combination of the factors of likelihood and severity defines the cell of the matrix in which a risk

lies, and each cell is assigned a rank. Risk rankings are used to define the acceptability and associated requirements for each risk.

The purpose of a risk matrix is to provide a method to enforce varying levels of acceptable risk based on the severity of an event and to allow a structured ranking of multiple risks associated with a change. An example risk matrix from the FAA Air Traffic Organization Safety Management System (ATO SMS) [11] is shown below in Figure 5-1. In this example, risk rankings are high, medium, and low depending upon the cell in which each risk is located. For catastrophic/ extremely improbable risks, there are two potential risk rankings: high if the outcome is the result of a single point failure, and medium otherwise. Risk matrices include severity criteria with associate events that indicate an increased likelihood of harm. These indicators do not have directly associated harm to people or property, especially for lower levels of severity.

Severity Likelihood	No Safety Effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote C					
Extremely Remote D					
Extremely Improbable E					*

High Risk
Medium Risk
Low Risk

* Unacceptable with Single Point and/or Common Cause Failures

Figure 5-1: An Example Risk Matrix from the FAA ATO SMS [11]

Based on ranking of risk, there can be different requirements associated with the acceptance of the risk. As an example, ATO SMS policy requires acceptance from multiple lines of business for initially high risks, while medium or low risks can be accepted by individual service unit managers [11]. It can also possible to require additional monitoring processes based on the ranking of risk.

The risk matrix approach is commonly used in many other aerospace standards. Examples are Eurocontrol safety guidance [55], SAE [31], and RTCA [30] safety assessment processes. The form of risk matrices, as well as severity and likelihood definitions vary between policies.

5.1.1 Hazard/Risk Identification

The risk matrix approach is typically structured around hazards. Organizing by hazard allows common behavior around a set of conditions to be analyzed, and simplifications made regarding the worst potential effects that follow from a hazard. Therefore, the initial step in the risk matrix approach is to identify hazards associated with a proposed change. The goal of hazard identification is to identify potentially dangerous states of operation to ensure that subsequent safety assessment activities are conducted for a sufficient set of safety behavior to ensure the safety of the change.

Hazard identification typically requires extensive understanding of many different types of system behavior. For systems-level changes, this includes knowledge of airborne systems, ground systems, procedures, and the expected operational environment. Committees of operational experts are typically involved to utilize their experience in assessment of past changes, and in conceiving of potential hazardous scenarios or failure modes.

Several methods facilitate hazard identification. Hazardous states based on failed components can be considered (known as forward search), or potential hazards arising from risks can be evaluated (known as backward search) [87]. Other techniques, such as scenario analysis [14] identify potentially dangerous operational conditions. The goal of utilizing several techniques is to develop a comprehensive list of hazards in the system, thereby ensuring completeness.

Risk events can also be identified at this stage. They are potential occurrences that result from events occurring after the hazard. As there are many potential events, there can be multiple risks associated with a hazard. This was illustrated using the hybrid bow tie representation in Section 4.3.1.

Hazard identification populates the rows of the influence matrix. This is illustrated in Figure 5-2 for identified hazards 1 to n . As illustrated, there can be unknown or uncontrollable hazards

associated with a change. This point is reinforced in Figure 5-2 by illustrating that the hazard identification process implicitly eliminates unknown and uncontrollable risks from scope.

Because identification depends on the experience of assessors, hazards are more likely to be identified if they have occurred in past system operations or similar systems. These two types of hazards are discussed in detail below. The lack of inclusion of unknown and uncontrollable hazards limits the scope of assessment even before formal scoping decisions are made.

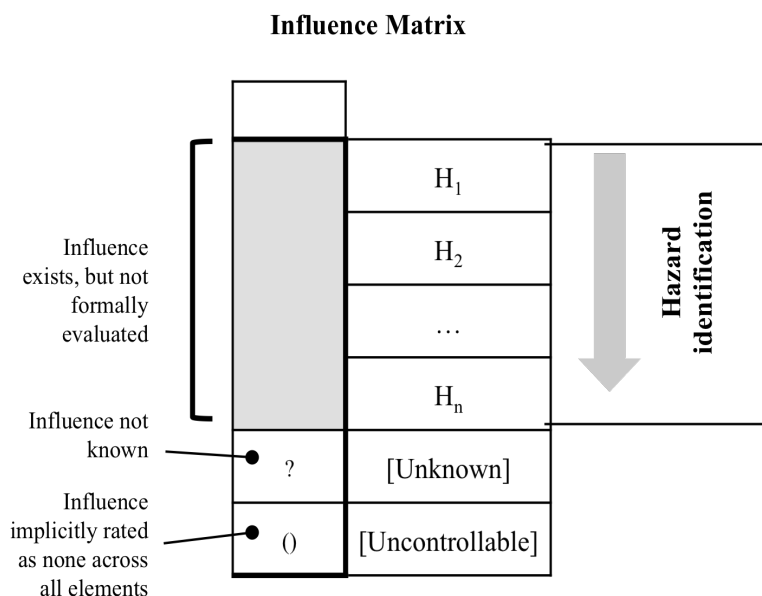


Figure 5-2: Hazard Identification

5.1.2 Scoping

The scoping process defines the depth and breadth of scope that must be included in the analysis of a proposed change. In the risk matrix approach, this requires identification of elements with significant influence on risks and hazards identified. In the initial stage, each hazard has multiple risks associated with it, and the influence of several system elements can be considered. This can result in a very large matrix describing the complete set of influence associated with the proposed change.

Based on the structure of the influence matrix, several strategies can be applied to limit scope, which will be discussed below. First, limiting scope through a dominant system state will be discussed. Similar to this approach is the use of dominant or stressing scenarios, as described in

Section 4.4.3. Next, scope limits inherent in acceptability criteria rankings are discussed. The final set of scoping strategies discussed is based on an examination of influence and elimination of low influence events from the scope of analysis.

Limiting Scope through the Worst Credible System State. Current ATO SMS guidance requires that the most severe risk associated with a hazard be assessed for the worst credible system state [11]. The worst credible system state is defined as follows:

Worst – The most unfavorable conditions expected (e.g., extremely high levels of traffic, extreme weather disruption). *Credible* – This implies that it is reasonable to expect the assumed combination of extreme conditions will occur within the operational lifetime of the change. The assessment should always consider the most critical phase of flight within which an aircraft could be affected by the failure under consideration. [11]
[emphasis in original]

One result of considering the worst credible system state is to scope out risks by dominance, as described in Section 4.4.3. By this logic, the worst state conditions associated with a hazard will result in the highest level of risk resulting from the hazard. Mitigating unacceptable risk levels under the worst credible conditions will then sufficiently mitigate risk level in all other operating conditions encountered.

A second result of scoping by worst credible behavior is to eliminate non-credible risks. Those events that are not reasonably expected to occur during the operation of the system are considered non-credible. This implicitly assigns a risk level that is within acceptability criteria to non-credible event sequences, thus making them negligible and scoped out of analysis.

Additionally, scoping by worst credible state can eliminate the effectiveness of mitigations applied to reduce risk. A hazard is defined for a set of conditions, of which one potential set is the worst credible conditions of operation of the system, and another set may be a similar hazard under less stressing conditions. This is illustrated conceptually for two hazards in Figure 5-3. The hazards have the same structure of initial causes and preceding events and would differ only in the probabilities assigned to events.

Four elements and two risks associated with the hazard are shown. In the example, Elements 1 and 2 (E_1 - E_2) influence the initial causes of the hazard. As shown in the bow tie model, these would influence the likelihood of the hazards. Elements 3 and 4 (E_3 - E_4) are mitigating elements,

influencing the likelihood of the branch in the event tree. They reduce risk level once a hazard has occurred.

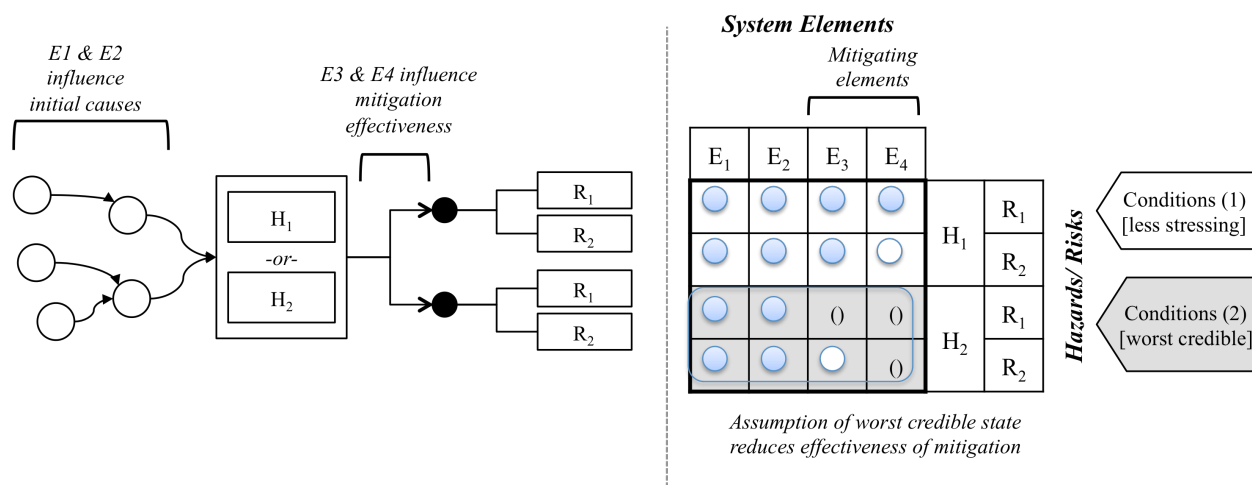


Figure 5-3: Reduction of Mitigation Effectiveness in Worst Credible System State

The mitigating elements are notionally assumed to be more effective in the less stressing condition, as shown by their magnitude of influence for Hazard 1 (H₁). When conditions are more stressing (e.g. the worst credible), the Element 4 (E₄) no longer has an influence, and the influence of the Element 3 (E₃) is reduced. Under the worst credible state, more stringent requirements would be placed on Elements 1 & 2 due to the reduced mitigation effectiveness.

Another effect of assuming the worst credible system state can be to strengthen the influence of one or several elements, because the hazard likelihood is correlated with the condition. This is shown notionally in Figure 5-4. Elements 2 & 3 (E₂-E₃) are shown with weak influence under the less stressing system state. Influence is weak because any change in their behavior has less of an effect on the risk level. The same elements are shown with strong influences under the more stressing system state, as changes to their behavior are more likely to increase risk level. An example of a condition that follows this pattern is the density of traffic. Aircraft are expected to have more conflicts as traffic density increases. Therefore all system elements that contribute to the occurrence of a proximity hazard would have a stronger influence under conditions of high traffic density compared to low traffic density.

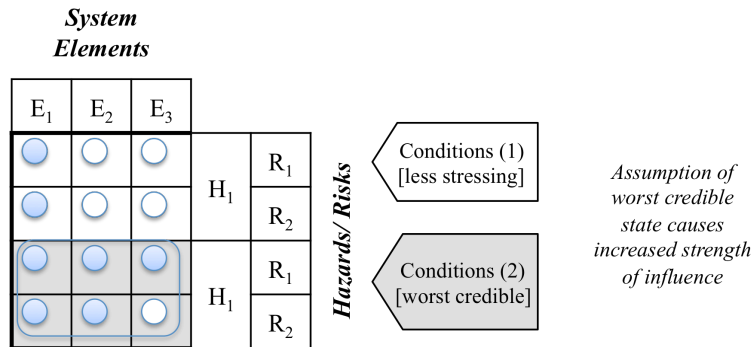


Figure 5-4: Correlation of Influence with Stressing Conditions

This scoping decision can have a significant effect on the validity of the assessed safety performance. It may be impossible to predict the worst case operating conditions, especially in the presence of dependent and interacting failures. This is especially for very low risk levels (e.g. 10^{-9}). The operational lifetime of a system required to ensure no expected events would be approximately 50 years, at the current rate of commercial airline operations¹¹.

Scoping analysis by assuming the worst credible system state may embed conservatism in the stringency of safety-derived requirements. The proposed change will not always operate in the worst credible system state. Therefore, on average, the risk level will be lower than assessed.

5.1.3 Detailed Assessment and Modeling/ Mitigation

In the detailed assessment and modeling process, expected risk levels and severity are evaluated for elements, conditions, and risks that have been identified as within the scope of analysis. Risks are then ranked by their location in the risk matrix. Unacceptable risks are addressed through mitigation. The detailed assessment process is typically performed to evaluate *initial risk levels*. These are the levels of risk associated with the proposed change without additional mitigations. This is the approach prescribed by the FAA Air Traffic Organization Safety Management System [11]. There are several methods used in detailed modeling and assessment. Two methods are discussed below. First, hazards can be assessed and mitigated independently of other hazards. Second, hazards can also be assessed as a group, resulting in evaluation of a subset of the scope of analysis.

¹¹ The NTSB reported 19 billion (1.9×10^7) flying hours for Part 121 carriers (airlines) in 2008. For constant operations, it would take 53 years for the entire airline fleet to reach 1×10^9 operating hours.

Assessing and Mitigating Hazards Independently. One strategy for assessing hazards is to decompose the influence matrix by hazard, assess risk, and determine mitigations for each hazard. This approach is illustrated in Figure 5-5. The scope of assessment is focused on a single hazard and associated risk in isolation. This is shown notionally for the third hazard/risk combination. The breadth of scope considers all elements with significant influence, with other elements scoped out of analysis. As shown, the scope includes only elements 1-4, although elements 1-6 influence other hazards.

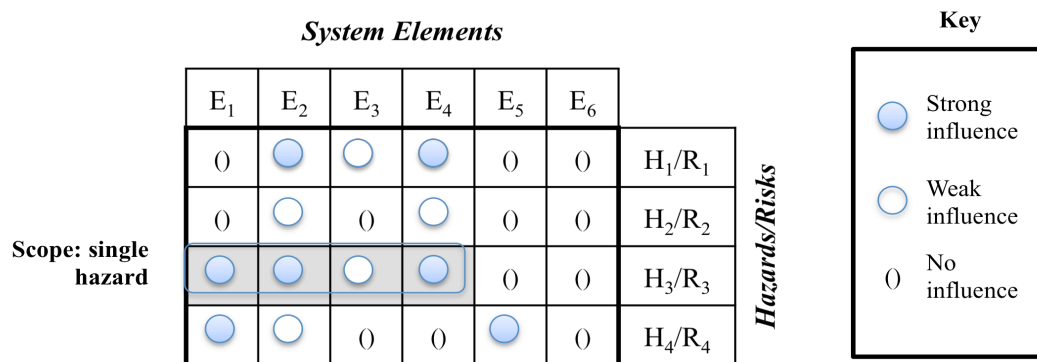


Figure 5-5: Single Hazard Assessment Decomposition

A potential challenge due to the decomposition by hazard is due to the practice not reassessing the proposed change after safety requirements have been derived. There is the potential that a mitigations derived for the system can reduce the risk level of associated with an individual hazard but increase the risk level of an additional hazard. Because of this potential, mitigations are commonly either designed to reduce risk levels under all potential conditions (i.e. all other hazards), or isolated to influence only the hazard under investigation.

The independent assessment of hazards also neglects the evaluation of tradeoffs in mitigations across hazards. Therefore, there is a risk that the approach can result in non-optimal system solutions. The system could be overspecified compared to a more holistic approach. The success of the approach is likely due to the fact that there are typically a small number of new requirements derived through the safety assessment process that substantially change the overall behavior of the system, allowing the influences to be isolated. As coupling increases, it may be more effective to group multiple hazards and risks together in assessment.

Assessing Hazards as a Group. When multiple hazards and system elements result from similar safety behavior, they can be grouped in analysis. These hazards would exhibit *clustering* in the influence matrix. A cluster of hazards is defined as hazards with a common set of system elements, with little or no influence of elements outside of the cluster. Clustering is typically a sign that the causal behavior of the hazards due is similar within the cluster. Clustering is notionally illustrated in Figure 5-6. There is a cluster of influence between Hazard/Risks 1 & 2 (H_1/R_1 & H_2/R_2) and Elements 2-4 (E_2-E_4). For these hazards, other elements do not exhibit an influence. For the other hazards shown (H_3-H_4), all system elements have influence and there is no readily apparent grouping.

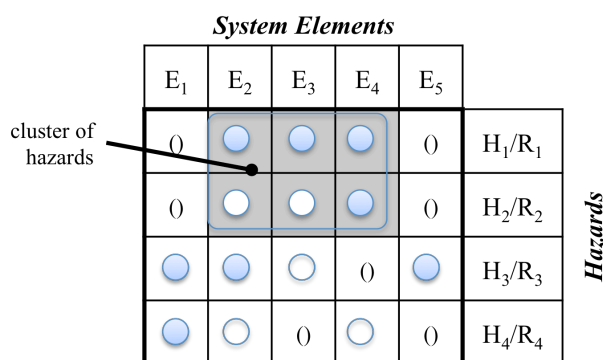


Figure 5-6: Evaluation of Groupings of Hazards (Clusters)

Grouped hazards in the influence matrix are necessary but not sufficient to define a cluster. In addition to having influence, the behavior that is exhibited to create the influence must also be similar. Similar behavior may arise when there are initial causes of hazards that originate from a subset of system elements, such as a specific set of avionics equipment. They may also be mitigated in similar forms, such as through training, or through the presence of a safety net (e.g. TCAS). By analyzing the hazards as a group, mitigation of similar behavior can also be considered as a group, resulting in a more holistic evaluation of tradeoffs between different mitigations strategies.

Form of Safety Models. Models used in detailed modeling in assessment can vary in form. Models can be qualitative or quantitative, and structured or unstructured. Qualitative estimation techniques classify likelihood in several categories that do not necessarily have a probability associated with them. In evaluating the expected behavior of the system, expert judgment is

used to assimilate all dynamics and assign likelihood. Qualitative methods tend to be unstructured and implicitly held by assessors. For significantly complex behavior, it can be difficult to rely only on unstructured models. Quantitative methods are typically used within a logical structure, such as a fault tree or an event tree that delineates potential state transitions leading to and from the hazard and estimates likelihood for each condition.

Models, particularly quantitative models, can be very complex and detailed. Complexity can arise from the need to incorporate complex causal behavior of risks or multiple conditions that are representative of expected operational experience. In many cases, quantitative models require relevant operational data to model component reliability, traffic characteristics, or to understand human performance in normal and degraded modes of operation.

The complexity of detailed models is a primary driver of the cost of the safety assessment process. Significant resources are required to compose complex model structures, obtain relevant data, and review key assumptions. There is a desire to keep models as simple as possible, to remain tractable, but sufficiently detailed to capture key safety behavior and remain credible.

5.2 Target Level of Safety Approach

Application of a Target Level of Safety (TLS) is effectively a subset of the risk matrix approach. In the approach, a risk level target is defined for a set of conditions (i.e. a hazard) that associated with a specific risk. The target is usually expressed in the rate of occurrence of events per unit of exposure (e.g. /hr or /departure). The target is decomposed from an overall risk event to a set of conditions for which analysis is conducted through a risk budget. The target is a threshold criterion. If the assessed risk level is below (i.e. less likely than) the target, the change is acceptable. If it is above (i.e. more likely than) the target, mitigations must be applied to reduce the risk. This risk budget scopes the hazard for which the proposed change will be assessed and allocates risk through conditions to the risk target. Thus, due to the nature of deriving a TLS, hazard/risk identification and scoping processes are inter-related. However, they will be discussed in separate sections. Following this, the processes of detailed modeling and assessment and mitigation will be discussed.

5.2.1 Hazard/Risk Identification

Creation of a Risk Budget. In the TLS approach, there is a need to determine how risk levels will be allocated hazards evaluated for assessment. This process is typically conducted using the methodology of a *risk budget*. This is illustrated conceptually in Figure 5-7. For a given risk associated with the proposed change, there are several hazards (shown as Hazards 1-n) that can result in the risk. Intermediate sets of conditions can be defined before arriving at hazards, but are not shown for simplicity.

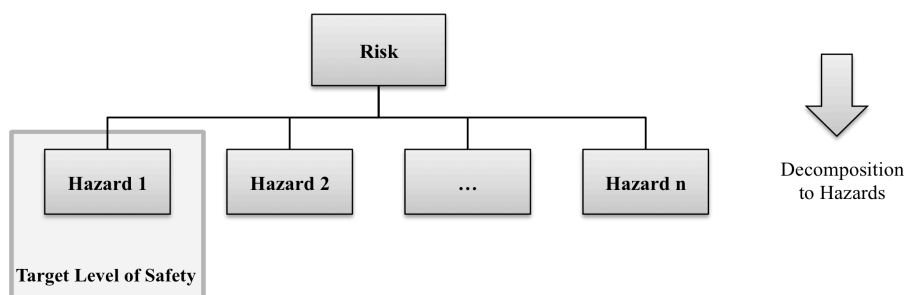


Figure 5-7: Risk Budget Decomposition of Hazards

Budgeting is performed to assign a target level of safety to the hazard that will be evaluated in safety assessment (shown as Hazard 1 above). Other hazards are typically scoped out of analysis, although it is also possible to use multiple risk budgets for a single system by defining multiple target levels of safety.

Hazards are defined based on conditions, which can be defined in several ways. One approach is to separate conditions based on types of exposure to risk. As an example, if the change is limited to enroute operations, safety can be evaluated separately for the enroute phase of flight (compared to approach and departure). By this approach, the sets of conditions would correspond to flight phases, and the condition of interest would be further decomposed to arrive at the target level of safety. Risk can also be budgeted to different causes of events. An example of this method is separating target levels of safety for normal performance of a system from that of failure conditions. When this is the case, a distribution of risk is enforced across multiple causes.

Determination of the Risk Goal. One of the issues in applying the TLS approach is determining the desired target for the top-level risk event, referred to here as the *risk goal*. This is set to enforce a goal on the risk level exhibited by the proposed change when it is implemented. There can be several approaches to setting the design target for the top-level risk event. These approaches are illustrated in Figure 5-8 and discussed below. These methods serve to enforce either equivalent levels of safety, or desired safety improvements in the system. From the total risk goal, the fraction of risk level at each level of decomposition of the risk budget is then determined.

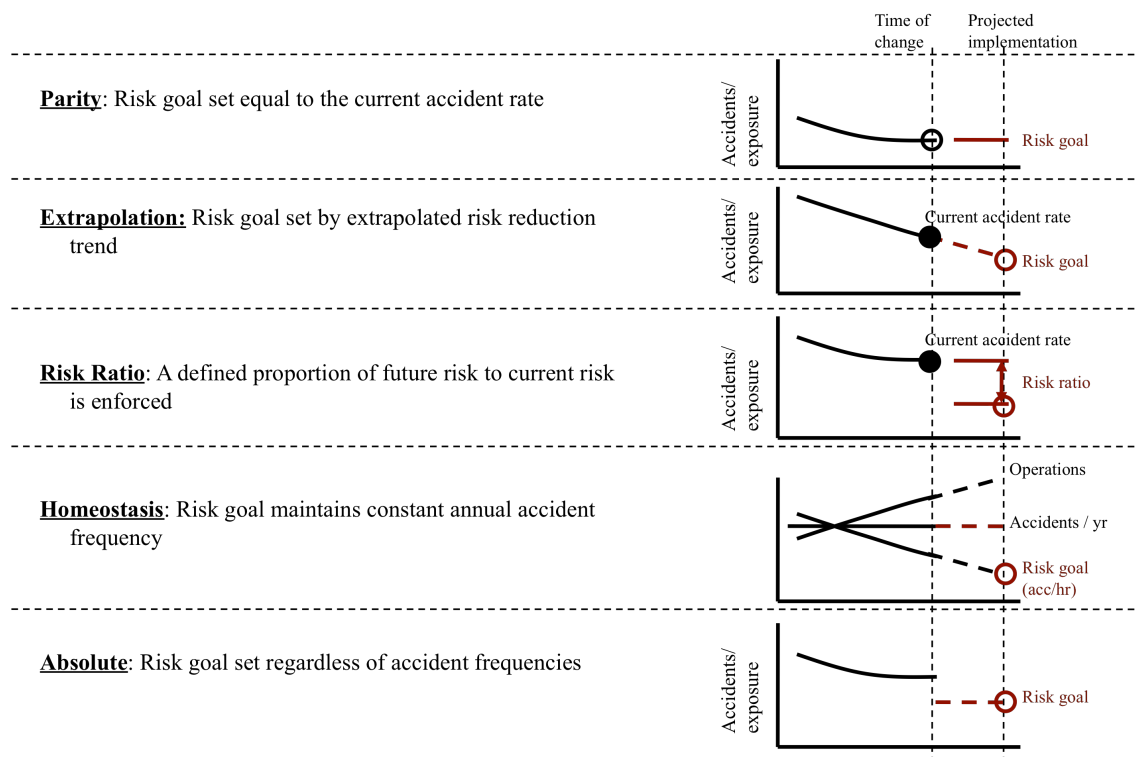


Figure 5-8: Methods for Setting Risk Goals

Parity. Using the parity approach, a representative analysis is used to estimate the current rate of accidents in the system. This analysis either averages accident rates over a time period up to the time of the change, or uses a point rate from a representative year. No additional improvement is required for the proposed change. It requires the new system to have an “equivalent level of safety” to the currently operational system.

Extrapolation. Recognizing the general trend of declining accident rates, one may expect the accident rate at a future date to be lower than the current accident rate at the time of implementing a proposed change. Under the extrapolation approach, the historical accident rate is extrapolated according to an observed trend line to an expected implementation date.

Risk ratio. The current accident rate may be unknown. If this is the case, a relative performance gain desired in the proposed change can be defined as a risk ratio. Evaluating a model of both the baseline system performance, and the system with the proposed change then allows a relative comparison of risk levels.

Homeostasis. Public perception of accident risk is typically assumed to be correlated with the annual frequency of accidents and not the accident rate [89]. This dynamic forms a mental model of regulators and policy-makers of a required static level of accidents per year. By this logic, increases in flying hours would increase the actual number of accidents per year. To keep that measure constant, a corresponding reduction in accident rates is required. The homeostasis approach is common in articulated policy goals for safety improvements [89].

Absolute. Absolute risk level targets set an accident rate threshold regardless of previous accident experience. This approach can be used to try to maintain consistent investment decisions across technologies or public harms. The absolute target level of safety includes the acceptability criteria in the risk matrix, as discussed in the previous section.

Budgeting the Risk Goal to Hazards. There are several potential approaches to budget the risk goal to hazards. Risk levels can be budgeted equally by hazard, which is typically performed when hazards are of similar severity. This assigns an equal weighting to the required performance of each hazard. Risk can also be budgeted by exposure, such that the risk goal is defined as an average level of risk in the operation of the system. Where available, operational data can also be used to budget risk levels to be equivalent to a proportion experienced in past operation.

5.2.2 Scoping

Risk budgeting decomposes risk levels to a design hazard. This has the effect of scoping analysis to the design hazard, with all other conditions in the risk budget outside of the scope of analysis. Applying the TLS approach requires influences of the design hazard to be decoupled from other hazards. This is the benefit of the TLS approach, that it focuses analysis on a set of decomposed elements and conditions.

This decoupling is illustrated conceptually in Figure 5-9. At the top of the figure, there is a risk that occurs under conditions 1 & 2. In this aggregate hazard, a given system element (E_1) is shown to have a strong influence on the occurrence of the hazard. However, the element's influence can be decomposed, such that it has a strong influence under the set of *Conditions 1*, but no influence under *Conditions 2*. For multiple elements in the system, using the TLS approach decouples their influence from other hazards and eliminates them from the scope of analysis.

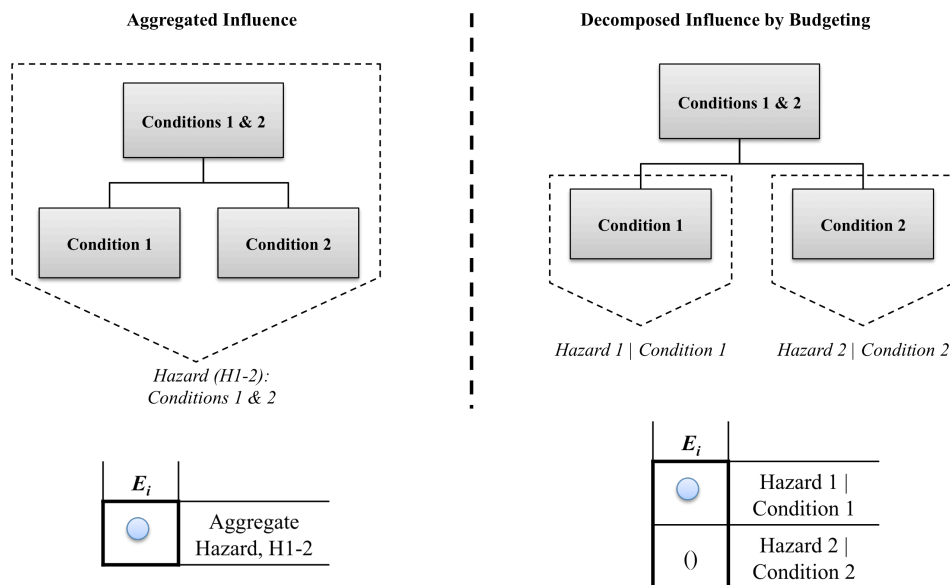


Figure 5-9: Disaggregation of Influence in Risk Budgeting

In the target level of safety approach, the basic assumption is that risk levels associated with hazards outside of scope are acceptable by similarity. The logic is that the overall influence of those elements, as it relates to the level of risk in the system is sufficiently similar to current

operation that they do not need to be evaluated in detail. This also requires the current system to be acceptably safe. Other risks or conditions as well as other behaviors that could influence them are judged to be out of scope.

The decomposition of influence by hazard is a significant assumption in the TLS approach. There can be uncertainty regarding the influence of changes to a system element on the risk level under other hazards. One example is the navigation paradox, initially identified by Machol [90]. The paradox is that as navigation precision is increased to reduce collision risk of adjacent aircraft in one dimension, collision risk can increase in other dimensions, which were scoped out of the analysis.

5.2.3 Detailed Assessment and Modeling/ Mitigation

Due to the quantitative definition of a target level of safety, quantitative models can be applied. This is in contrast to modeling in the risk matrix approach, which uses both qualitative and quantitative methods. The emphasis on quantitative modeling typically results in the use of the TLS approach to set requirements for technical performance measures. The TLS approach can also be used to evaluate the behavior of multiple interacting components through simulation methods, such as Monte Carlo analysis.

One method of application of the TLS approach is to separate a risk target for normal performance from failure conditions. This approach is appropriate in cases where technical performance of the system under normal operation correlates strongly with risk. An example is the relationship between navigation accuracy and midair collision risk. When this is the case, the properties of change elements are typically set to meet acceptable safety targets based on the risk model used.

With target levels of safety derived for midair and ground collision risks on the order of 10^{-7} and 10^{-9} events/hr, high safety performance of change elements can be required. Data underlying performance at very low likelihood levels is typically not observable at the level of fidelity required to support assumptions on probability distributions. Instead, causal models are used to model relevant parameters and fit appropriate probability distributions that extend performance beyond observed data.

5.3 Performance-Based Approach

For a class of proposed changes where there is similar functionality in a currently operating system, safety requirements can be derived through the comparison to a reference system. The performance-based approach has been specifically recognized as acceptable by the International Civil Aviation Organization (ICAO) for approval of systems that influence airborne separation [8]. The ICAO approach is one example of the more general set of equivalence methods.

Applying the performance-based approach requires the identification of a suitable reference system that has been judged to be safe either through analysis or through operational use. Given the selection of a suitable reference system, there are two steps required to derive safety requirements of a proposed change using the reference system. The first is to select relevant performance measures that characterize the performance of the reference system. Tradeoffs can then be evaluated along these performance parameters in deriving safety requirements. The second process is to evaluate operational differences between the reference system and the proposed system. These differences must be mitigated such that they do not degrade safety.

5.3.1 Hazard/Risk Identification

In the performance-based approach, hazards and risks are not identified directly. Instead, it is implicitly assumed that hazards and risks will not change.

5.3.2 Scoping

The scoping process within the performance-based approach is performed to separate two sets of elements: those characterized by performance measures, and those that represent other operational changes. These can be illustrated using the influence matrix framework in Figure 5-10. A set of aggregate performance measures is identified to characterize both the reference system and the proposed change. For the elements that contribute to these performance measures (E_1 - E_3), changes do not have an influence on risk level. For some operational change elements, there will be an influence on risks associated with the change. An example could be new procedures introduced that were not present in the reference system. This is shown by notionally assigned influences for Elements 4-6 (E_4 - E_6). The reference system approach requires operational change elements to be specified such that they do not increase risk. There will also

be other elements in the external system and proposed change that are judged sufficiently similar that they are scoped out of analysis that are not shown in the figure.

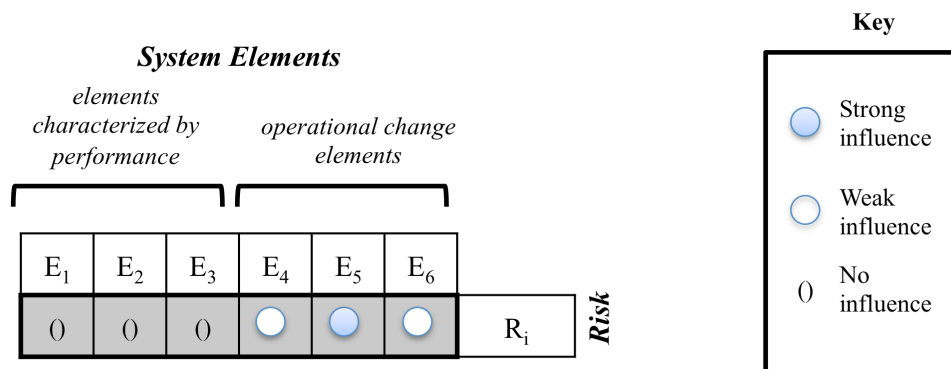


Figure 5-10: Influence in the Performance-Based Approach

5.3.3 Detailed Modeling and Assessment

The analysis of aggregate performance measures in the performance-based approach is illustrated in Figure 5-11. Aggregate performance measures are identified that characterize the safety of the reference system. These serve to judge the performance of the proposed change. Modeling and assessment may be performed to evaluate tradeoffs between individual performance parameters that result in the same aggregate level of performance. Once these performance measures are derived, they are then specified as requirements for the proposed change.

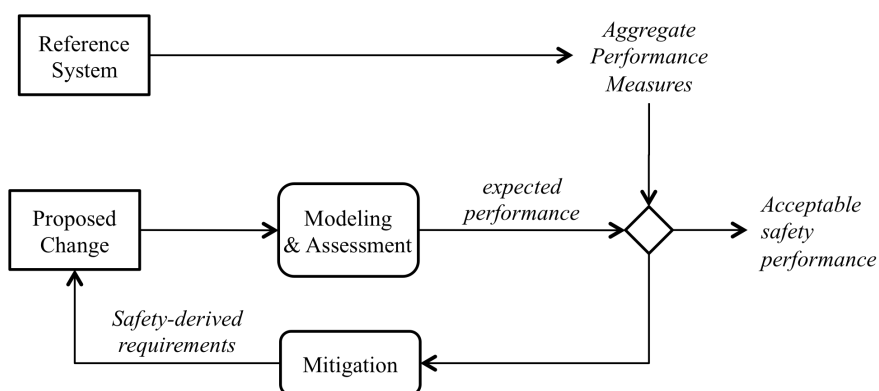


Figure 5-11: Illustration of the Performance-Based Approach

Some operational elements can differ from the reference system. These are not evaluated to risk or performance criteria, but are specified as part of the proposed change such that they do not

increase risk. Based on the goal of maintaining an equivalent level of safety, any increase in risk level due to operational elements is mitigated for each element.

The performance measures selected for the reference system are commonly technical measures of performance for which tradeoffs can be measured. These technical parameters include accuracy of position in different dimensions, integrity (guarantee of position to a given level of fidelity), latency, and availability. As such, assessment using the reference system method is appropriate for a limited class of changes where these technical parameters can be used to define the system. These include surveillance and communication systems.

The performance-based approach is limited to very similar applications to current system operation and can therefore only deliver the same level of functionality. It cannot be used with when operational elements have significant influence risk levels that are not similar in causality to those in the current system. These would include large reductions in separation, changes in task allocation, or new functions performed by the change.

6 Application of Influence framework to Safety Assessment of European Reduced Vertical Separation Minima

To test the influence matrix framework developed in this work, it was applied to the documented safety assessment of Reduced Vertical Separation Minima (RVSM) in Europe, which was one of the eight cases analyzed. This chapter documents the application of the influence matrix, the identification of scope decisions made, and the consistency of scoping decisions with a subsequent analysis of RVSM performed. The chapter begins with an overview and description of RVSM. This is followed by a discussion of the safety assessment methods used and associated documentation. Next, the influence matrix based on the RVSM safety assessment is presented, along with a discussion of the key scoping decisions that can be identified from the framework. The chapter concludes with a discussion of the implications of the scoping strategies applied for the safety of implemented RVSM.

6.1 Overview and System Description of RVSM

Under conventional separation minima, aircraft are separated vertically by 1,000 ft flight levels (FL) below FL 290 (29,000 ft) and by 2000 ft. above FL 290. The increase in vertical separation with altitude has been required due to the sensitivity of altimeters that rely on pressure measurement. At higher altitudes, the same change in pressure measurement translates to a greater change in altitude. This is shown in Figure 6-1 for two example points: 1) at 5,000 ft and 2) at 30,000 ft (FL 300). The slope of the pressure curve is greater for the second point. Therefore, for a fixed sensitivity in pressure measurement, there is a large altitude error with increasing altitude.

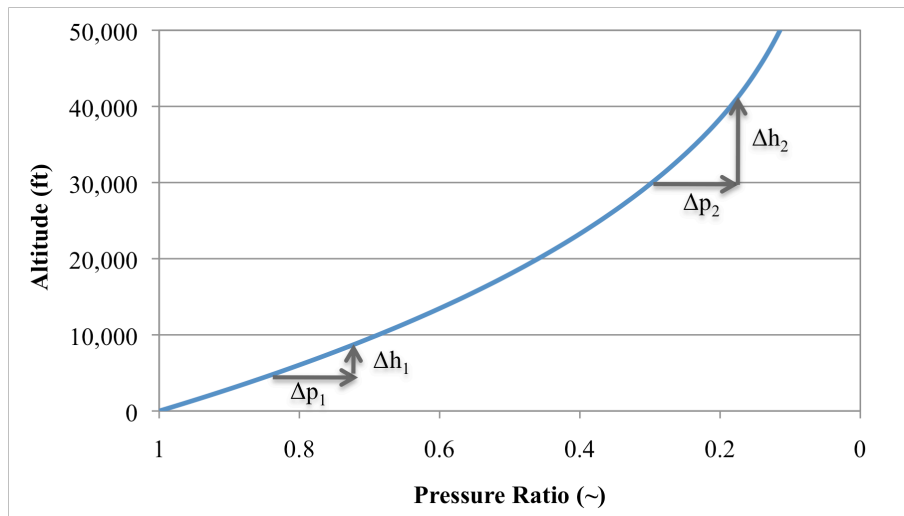


Figure 6-1: Variation of Pressure with Altitude

Improvements in altimetry precision made it possible to reduce vertical separations at higher altitudes. Beginning in 1990, ICAO published draft guidance material [91], on the feasibility of reducing vertical separation in several regions. Altimetry performance was assured through certification to Minimum Aviation System Performance Standards (MASPS) on new and retrofit altimetry systems.

RVSM added six additional flight levels, by reducing vertical separation from 2,000 to 1,000 ft between FL 290 and FL 410, as shown in Figure 6-2. The increase in available cruising altitudes enabled more efficient operations and additional capacity.



Figure 6-2: Additional RVSM Flight Levels [92]

From 1997 to 1998, RVSM was implemented in the ICAO North Atlantic Region [93]. Following this implementation, Eurocontrol performed a safety assessment supporting implementation in the European region (EUR). This safety assessment was conducted for the specific EUR operational environment, but built on standards on aircraft performance that were established earlier by ICAO. The change was approved and implemented in EUR airspace in 2002. RVSM has also been implemented in most other regions, including the United States, but those implementations are not the focus of this analysis.

To support operational approval in the European Region (EUR), two safety assessments were performed, both before [94] and after [95] implementation. Each safety case considered transition areas to RVSM, and “core” RVSM airspace. The focus of this case study is on the assessment of mature airspace performed in the Pre-Implementation Safety Case (PISC) [94]. As part of the safety case, a Functional Hazard Assessment (FHA) was also conducted [92].

The discussion of this case will begin with a description of the safety assessment approaches used. Analysis of the case is then organized along the general processes of safety assessment: hazard identification and scoping, detailed analysis and modeling/ mitigation, and operational approval.

6.2 RVSM Safety Assessment Approach

RVSM provides interesting insight to two methods of analysis. The safety assessment utilized both the Target Level of Safety (TLS) approach and the risk matrix approach. Both approaches were combined to support the safety argument using goal structuring notation (GSN). GSN is a formalism for supporting logical arguments regarding the validity of the safety case. The TLS was used as a basis for acceptability of collision risk assessments of the effect of operational errors and altimetry performance on loss of vertical separation. Additionally, a failure hazard assessment (FHA) was conducted, and risks were mitigated to risk matrix acceptability criteria. The FHA was performed according to EU guidance [55]. The documentation of the FHA was sufficient to identify the influences of system elements on associated hazards as identified by the safety assessors. It documented the rationale for initial risk levels derived, and the effect of mitigations derived to achieve acceptable levels of risk.

Brief Discussion of the RVSM TLS and Risk Budget. The ICAO Review of the General Concept of Separation Panel (RGCSP) established the TLS used for RVSM. The panel set the Target Level of Safety in vertical separation as 5×10^{-9} accidents per flight hour [96] using a risk budget, which is illustrated in Figure 6-3. The historical rates of fatal accidents, en-route accidents, and midair collisions were reviewed, and the overall risk goal for each category was set to be equivalent to current operation.

From the historical midair collision risk of 1.5×10^{-8} accidents / hr, risk was budgeted equally to each dimension of flight. Loss of planned separation in the vertical, longitudinal, and lateral dimensions were treated as separate, independent events, and the overall risk budget for a midair collision was divided into thirds for each dimension. This resulted in a target of 5×10^{-9} accidents/hr due to loss of planned separation in the vertical dimension. Half of the rate was budgeted to technical height-keeping performance and the other half to other hazards (such as operational errors).

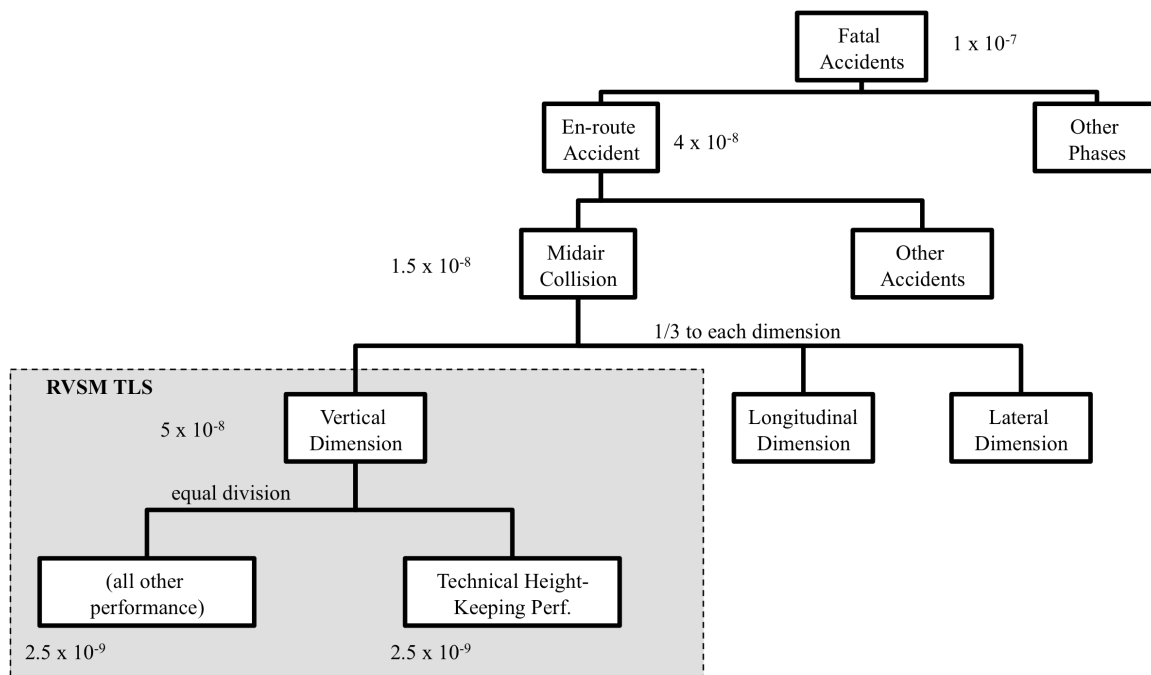


Figure 6-3: TLS Decomposition for RVSM

6.3 Application of the Influence Framework to the RVSM FHA

The documentation of the FHA [92] performed for RVSM describes the process of hazard identification, scoping, and risk assessment in sufficient detail to provide a basis for retrospectively applying the influence matrix framework. An influence matrix was constructed based on the published FHA. The influence matrix provides additional insight into decisions made during the hazard assessment. Of particular insight is the analysis of several subdivisions of scope that involved common mitigations and hazards. The discussion below will highlight several decisions made in the FHA using the influence matrix, the process for constructing the influence matrix, and the associated identification of groupings of hazards.

6.3.1 Methodology Applied to Create the RVSM Influence Matrix

The FHA for RVSM was conducted by hazard (as opposed to by risk). Each hazard is a set of conditions that could result in harm. Thus, identification of hazard identified potentially dangerous conditions that were of concern. Each set of conditions could result in several risk events. For each hazard, the worst credible effect occurring after the hazard was used to define the risk event. The severity and risk level of each risk event are then used to rank each hazard in the risk matrix.

In the assessment of RVSM hazards, operational experts developed an initial list of hazards through a structured process of eliciting operational hazards. Hazards were grouped into three areas: during switchover (i.e. the operational change from conventional to reduced separation minima), in transition airspace (borders of the region where conventional separation is applied), and in core airspace. The influence framework application was limited to hazards associated with core airspace, under the assumption that this would be the mature operating state of the system. This limits hazard conditions to those related to mature, core airspace.

The hazards identified are arranged in rows of the influence matrix. As shown in Figure 6-4, the RVSM assessors identified 26 hazards, after the elimination of duplicate hazards. Implicit in the process is the elimination of uncontrollable hazards, such as meteor strikes, which were not considered.
















































No.	Hazards	System Elements					
		Airspace	Flight Crew	Aircraft Equipment	ATC Equip	ATC Operator	TCAS
1.3	System error – altitude deviation				0	0	0
1.14	Change of approval status during flight (downgraded). Pilot will not be able to control level		0		0	0	0
1.15	Air RX/TX unserviceable [radio]	0			0	0	0
1.2	Nuisance TAs and RAs			0	0	0	
1.8	'Pilot is deviating from clearance'				0	0	
1.6	The pilot will miss the visual perspective of other traffic from the flight deck and will deviate from cleared level/track			0	0	0	0
1.9	Aircraft unexpectedly encounters turbulence that affects RVSM operation			0	0	0	0
1.11	Sudden deviation from cleared FL and/or route [due to wake]			0	0	0	0
2.2	'W' in indicated in the flight plan or the pilot claims aircraft for RVSM approved despite this is not the case			0			0
2.4	Flight plan totally missing	0		0			0
2.7	RVSM status of aircraft operating immediately above and below RVSM airspace not known to ATCO	0		0		0	0
2.23	"STCA not reacting correctly when RVSM is temporarily suspended and increased VSM is introduced"		0	0		0	0
2.6	STCA functionality not able to discriminate between RVSM approved aircraft and non-RVSM approved aircraft	0	0	0		0	0
2.8	Missing IFPS checks of FPLs [flight plan] coming from states inside RVSM	0	0	0		0	0
2.9	The manual insertion of changes or missing RVSM approval status	0	0	0	0		0
2.1	ATC systems are not able to exchange OLDI messages containing data about RVSM approval status	0	0	0		0	0
2.11	ATC systems are not able to internally distribute data about RVSM approval status	0	0	0		0	0
2.13	RVSM status has to be transmitted manually to succeeding unit, if information is missing on flight plans	0	0	0		0	0
2.5	Potential loss of separation due to wrong application of separation standard for OAT and GAT [public a/c]		0	0	0		
2.17	ATCO issued incorrect clearance	0	0	0	0		
2.27	Computer failures	0	0	0			
1.16	"Non-RVSM approved aircraft flying above FL410 and performs emergency descent"			0	0	0	0
2.12	"Different co-ordination requirements with different MIL agencies within the ACC"	0	0	0	0	0	0
2.21	"Definition of vertical dimensions of TRAs may differ from state to state"	0	0	0	0	0	0
2.25	"Ground TX/RX [radio] unserviceable"	0	0	0	0	0	0
1.1	Aircraft with MTOW < 15.000kg or <30 pax might not be carrying ACAS 7.00	0	0	0	0	0	0

Figure 6-4: RVSM Influence Matrix with Identified Clusters

The assessors also recognized five categories of system elements: airspace design, flight crew, aircraft equipment, ATC equipment, and ATC operators. Each element served as a category for which safety requirements were derived. Thus, these divisions of elements were used to populate the influence matrix and categorize influence. In addition, risk levels were also influenced by the interaction of RVSM with existing TCAS equipage. Although not explicitly identified as a system element, the behavior of TCAS influences risk levels, so the system was added as a sixth system element.

In the FHA process, participants did not explicitly analyze hazards using the influence framework. However, the FHA documentation explains the rationale used to assess the risk levels associated with hazards, and to derive required mitigations. Within this rationale, there is discussion of the influence of each element on risk, and how that influence is mitigated to achieve acceptable safety levels. This provides a basis for coding the magnitude of influence based on the documented rationale.

When a property of a system element contributed directly to the behavior resulting in a hazard's risk level, it was coded as a strong influence. Direct contributions were consistent with language stating that the system element directly caused the risk associated with a hazard, through multiple failure modes or causes related to the behavior of that element. As an example, the influence of flight crew on the hazard "pilot is deviating from clearance" is coded as strong. The FHA recognizes multiple flight crew causes that may cause a pilot to deviate from clearance, such as call sign confusion or errors in programming of flight automation.

When a system element was indirectly related to the risk level of a hazard, it was coded as weak. This is the case when the additional element interacts with functions performed by other strong elements, or has small changes in behavior as a result of RVSM. For the same hazard above, airspace design was coded as a weak influence. The changes due to RVSM change the likelihood that an error by the flight crew or controller will result in a loss of separation. The reduced distance between flight levels reduces the amount of time before a conflict can be recognized and corrected.

When a system element was not mentioned, and was logically not expected to influence risk, the influence was rated as none. There are four hazards shown where no elements influence the hazard. These were recognized by the assessors as hazards that currently exist, for which no changes to RVSM influence the risk of the outcome. By this assumption, the hazards were scoped out of detailed analysis.

Continuing the coding process for each hazard, the influence matrix was filled. After this process, hazards were grouped and reordered for common influence mechanisms, resulting in clusters. This is discussed in the following section.

6.3.2 Scoping in the RVSM Influence Matrix

Implicit in the FHA process was the exclusion of scope of four hazards present in the RVSM concept, but were uncontrollable through requirements derived on changes to RVSM system elements. The first two hazards excluded related to existing airspace coordination issues (Hazards 2.12 and 2.21). The second is the potential for unequipped TCAS aircraft (Hazard 1.1), for which equipage rates could not be enforced along with RVSM changes. The third and final hazard was related to the failure of ground-based ATC communication (Hazard 2.25). All of the above hazards were deemed to be uncontrollable. It was the judgment in the FHA that no RVSM system element's behavior could be changed to either increase or decrease the risk of each hazard in implementation. Related to this premise was that these hazards were already qualified by similarity. They existed in current system operation and were mitigated. This is reflected with the absence of influence of any system elements on the hazards.

Although it was recognized that there were strong interactions influencing RVSM hazards, TCAS was also scoped out of the analysis. The argument was based on similarity, under the rationale that TCAS was routinely used at lower altitude levels and was acceptably safe, and behavior could be expected to be similar in the implementation of RVSM. As will be discussed later, limitations of this assumption were recognized and a monitoring program was used to identify and correct risks related to TCAS interaction. The influence matrix illustrates the implications of this scope decision.

Identification of Clusters. A cluster is a set of system elements and hazards that have similar influence and safety behavior. It is represented in the influence matrix by a localized grouping of common influence across hazards and risks. Nine clusters were identified from the RVSM influence matrix. Clusters were initially identified by rearranging the influence matrix to group hazards together by the system elements that influenced them. This process resulted in several groups where a subset of system elements influenced each hazard and the remainder exerted no influence. From the initial groups, the narrative for each hazard contained in the FHA was examined to determine if elements contributed to hazards through similar behavior. Where this was the case, the set of elements and hazards indicated a cluster.

Within a cluster, the hazards, elements, and associated safety behavior were sufficiently similar that the hazards could be mitigated together through common mitigations. This clustering approach was not explicitly followed in the FHA process, but represents a potential method for examining grouped behavior that may have been performed implicitly by the assessors.

The resulting clusters identified are shown in Figure 6-4, indicated by rounded boxes. Each cluster is numbered and discussed below. Where elements within each cluster are not adjacent, the labels are divided by letter or by a dashed line to an individual element. The clusters identified are consistent with a subsequent review of the FHA as discussed in the following section.

Cluster 1: altitude deviation due to a system error. This cluster is associated with a single hazard. The “system error” refers to a failure in the aircraft altimetry system that could reduce separation. This cluster was analyzed through a collision risk assessment conducted to derive altimetry system performance.

Cluster 2: anomalous aircraft equipment performance. This single hazard is associated with aircraft equipment failures that can result in loss of RVSM capability. The hazard was addressed with procedural mitigations.

Cluster 3: nuisance TAs and RAs is heavily influenced by interactions between RVSM and TCAS. TCAS behavior has a strong influence on pilot deviation from altitude, and on pilot

reactions to nuisance TAs and RAs. The two hazards were determined to be the most safety-critical (i.e. the highest ranked associated risks) in the RVSM FHA. They were not adequately mitigated, and TCAS was scoped out of the analysis. This decision required additional monitoring processes after implementation to ensure risk was acceptable [97].

Cluster 4: pilot deviation from flight level contains multiple hazards related to potential pilot errors that result in altitude deviations. The consequences of errors were evaluated by examining past reports of altitude deviations. Behavior was expected to be sufficiently similar that the implications of the deviations with reduced flight level separation were expected to be acceptable using similar mitigating approaches. In addition, several requirements were derived related to flight crew training.

Cluster 5: ATC system accommodation of RVSM functionality represents the consideration of air traffic control equipment design to introduce functionality required due to implementation of RVSM, such as different flight plan inputs. Mitigations of the hazards were based on best practices and judgment to assure the functional operation of the system.

Cluster 6: Incorrect clearance by ATC (between RVSM/ conventional); Cluster 7: computer failures; Cluster 8: Non-RVSM emergency descent. Clusters 6-8 were not examined in significant detail in the FHA. Cluster 6 contains hazards related to controller operational errors. These were mitigated through controller requirements. Cluster 7 was addressed through the implementation of ground-based system requirements on reliability and software assurance. Cluster 8 pertains to an emergency scenario, and best practices were used to implement appropriate procedures.

Cluster 9: existing hazards in reference system. This cluster is noteworthy due to the lack of influence of any system elements. All hazards within the category were judged either to be out of scope (not related to RVSM) or sufficiently similar to current operations that no design changes evaluated would influence the risk. They were therefore scoped out of the analysis.

In the preceding analysis, clusters were identified retrospectively. In future assessments, identification of clusters can enable the integrated assessment of mitigation strategies. These mitigations strategies are likely to be more effective at mitigating hazards with common causal

behavior in comparison to individual mitigation of each hazard, because they enable to analysis of combined effects of the mitigation.

6.3.3 Subsequent Review of FHA Hazards

After RVSM implementation, Eurocontrol conducted a Post-Implementation Safety (POSC) [95], updating the initial assessment of RVSM hazards with operational data and results from monitoring. As part of the POSC, a review of the initial FHA was conducted [98]. The review was conducted in light of three identified challenges in the initial FHA: 1) the assessment of each hazard individually neglected aggregate risk levels from all hazards, 2) hazards were closer in definition to causes, making them “remote” from the risk event, and 3) to risks were found to be high, contrary to operator expectations [95].

It is interesting to note that the clusters identified above address concerns identified in the subsequent review. The correspondence between hazards defined in the FHA review and clusters is discussed below, after an introduction to the hazards identified in the FHA review. Hazards in the review were based on a functional model of RVSM shown in Figure 6-5, and there were nine subsystem hazards that contribute to an overall hazard of the aircraft being on the wrong flight level or route.

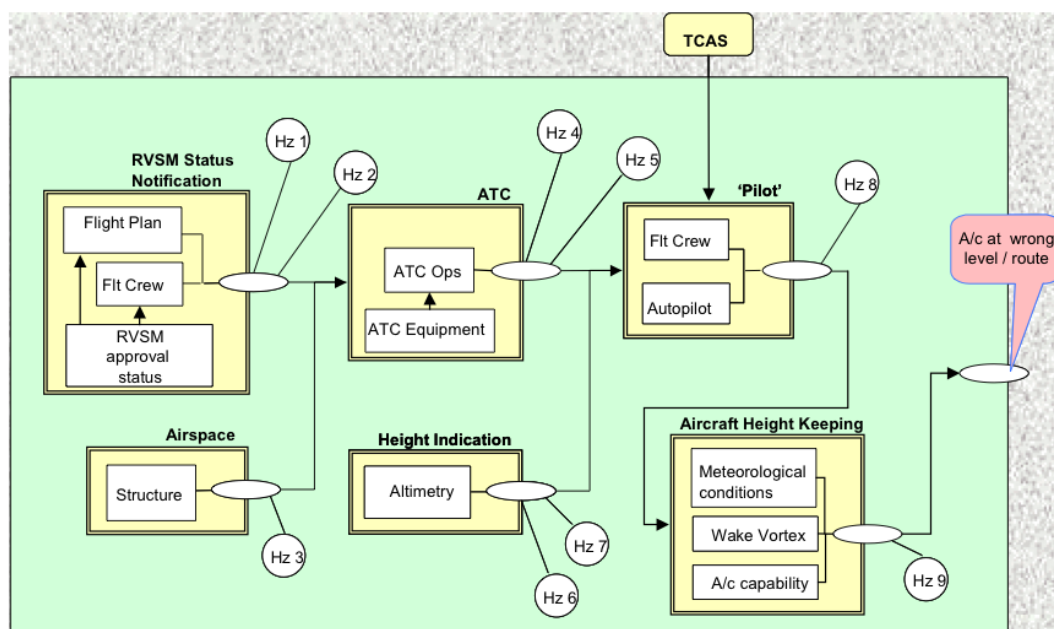


Figure 6-5: RVSM System and Subsystem Hazards [98]

The subsystem hazards identified were [98]:

1. Non-RVSM approved aircraft is indicated as RVSM approved
2. RVSM approved aircraft cannot indicate loss of RVSM capability to ATC
3. Airspace structure is wrong
4. Aircraft is assigned inappropriate level and/or route
5. No clearances / instructions are given to pilot from ATC
6. Undetectable altimetry system error
7. Loss of, or detectable error in, altimetry information
8. 'Pilot' deviates from cleared level and/or route
9. Aircraft is unable to maintain cleared level

Although a reassessment of combined influence was not possible from the structure of the review report, the hazards identified in the review are generally consistent with the insights gained from the identified clusters found using the influence matrix. Differences and similarities found between the two approaches are shown in Figure 6-6. Clusters identified using the influence matrix are shown in the first column, and hazards from the subsequent review are shown in the second. When clusters are related to hazards, they are linked in the figure. Those without links do not relate. In the discussion that follows, the terms clusters and hazards will be used to differentiate the two columns.

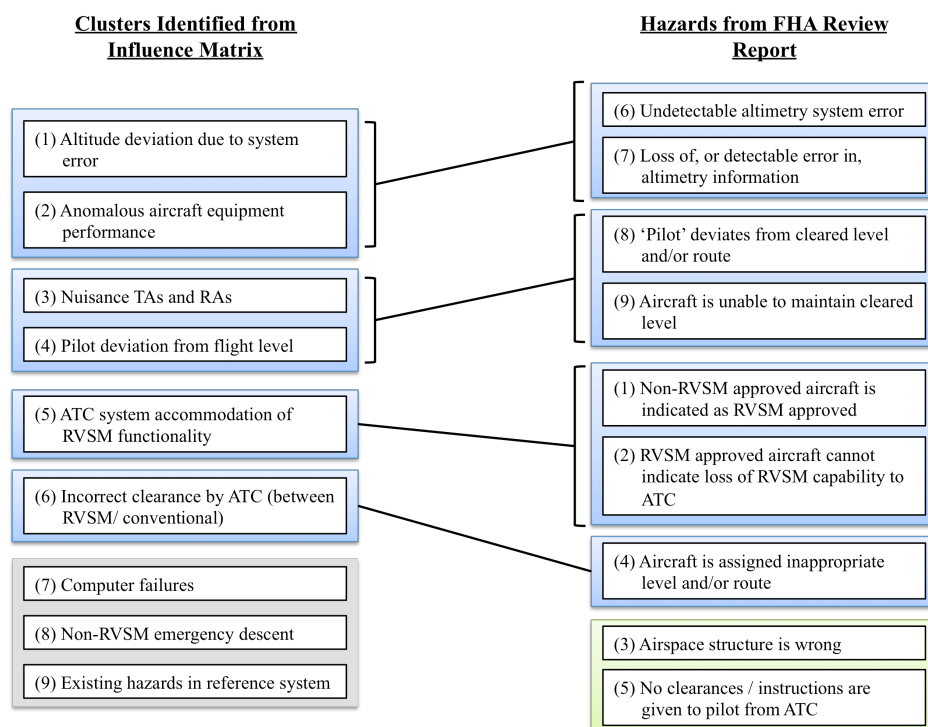


Figure 6-6: Comparison of Influence Matrix Clusters to Review Report Hazards

As can be seen in the figure, in the first two relationships, multiple clusters correspond to multiple hazards. In the third relationship, a cluster corresponds to two hazards, and in the fourth relationship, one cluster corresponds to one hazard. The remaining hazards and clusters do not relate.

In the first relationship, Clusters 1 and 2, relate to two review hazards (Hazards 6 & 7). These linked hazards and clusters describe the effects of failures in aircraft equipment that influence altitude. The clustering analysis separated deviations due to system errors and other aircraft equipment failures. The hazards separate the same concerns undetectable and detectable errors in altimetry performance.

Clusters 3 and 4 describe behavior related to altitude deviations, and correspond with Hazards 8 and 9. Corresponding hazards are broken down into whether deviation was intentional or uncontrollable. These clusters include strong influence of TCAS behavior in corresponding risks. In the initial assessment, the interaction with TCAS caused the risks to be ranked high, requiring additional monitoring. The review report recognized operational experience with pilot deviations TCAS performance to judge that the corresponding hazards were safe.

In the third relationship, Cluster 5 corresponds with two hazards (1 and 2). Cluster 5 incorporates hazards due to a failure of ATC systems to accommodate RVSM. The corresponding hazards divided this into two separate types of hazard: a) related to non-RVSM aircraft being approved in RVSM airspace, and b) indication of loss of RVSM to ATC. Other behavior in the cluster related to flight planning inputs was not recognized in the review report. The review report was focused on operational hazards, and this cluster was mitigated through best practices in design.

The final relationship identified was straightforward. Cluster 5 is equivalent to Hazard 4, and describes an inappropriate clearance for the type of aircraft cleared (e.g. non-RVSM aircraft cleared on RVSM route).

Several clusters were not included in the hazards of the review report, such as ATC computer failures (Cluster 7), emergency descent of non-RVSM aircraft (Cluster 8) and the cluster of

behavior that was scoped out of the initial analysis (Cluster 9). These were either judged to be low-level causes of other hazards, or were appropriately scoped out (in the case of cluster 9).

Finally, the review report added two hazards. Hazard 3 related to airspace structure, which was validated by the entire pre-implementation safety case. This was likely inappropriate to identify as a hazard in the review case, as it would be the cause of other hazards. The influence matrix captures this through the “airspace design” system element. This indicates hazards where the structure of the airspace design contributes to the risk level. Hazard 5 was also added, but is solely related to transition airspace, which was scoped out of this analysis.

6.4 Summary

The influence matrix provided valuable insight when applied to the pre-implementation safety case arguments. Clustering of hazards identified cases where common behavior contributed to similar risks. Assessing risk and designing mitigations for each cluster enables a more integrated approach to determining requirements. These approaches were identified in the subsequent published review of the FHA.

Several of the identified clusters directly correspond with aggregated hazards identified in the review report. These indicate hazards that were initially defined in a manner too similar to causes. Because of this, the structure of influence of potential mitigations in the influence matrix is common, which indicates that all elements can mitigate the causes in a similar manner. By clustering these hazards, they are redefined at a more appropriate level that allows mitigations to be examined in an integrated fashion.

The influence framework also identified significant interactions between TCAS and RVSM changes that affected risk levels. These were the focus of extensive reassessment in the review report. The conclusions from the reassessment, however, may not have been available before implementation, as they relied upon on RVSM operational experience. Therefore, the benefit of the influence matrix was in characterizing a concern that was identified by assessors and providing justification for the need for monitoring.

7 Challenges in Safety Assessment Identified from Case Studies and Implications for Safety Assessment of Future Systems-Level Changes

Several trends and challenges in safety assessment were identified through case studies performed and documented in Appendix D. Cases were selected that implemented operational changes to the air transportation system with documented safety assessment. Eight cases of systems-level change were analyzed. Six of the changes have been implemented and two are pending. A summary of the case studies analyzed is shown in Table 7-1.

Table 7-1: Summary of Case Studies Analyzed

System-Level Change	Implemented Year	Assessment Methods
Instrument Landing Systems (ILS)	1961	TLS
North Atlantic Organized Track System (NAT OTS)	1966-1981	TLS
Traffic Alert and Collision Avoidance System (TCAS)	1993	TLS (Risk Ratio)
Precision Runway Monitor (PRM)	1997	TLS
Automatic Dependent Surveillance, Broadcast (ADS-B) Alaska Capstone	1999	Risk Matrix
EUR Reduced Vertical Separation Minima (RVSM)	2002	Risk Matrix TLS
Automatic Dependent Surveillance, Broadcast (ADS-B) Segments I and II	(pending)	Risk Matrix TLS Performance-Based
Unmanned Aircraft Systems (UAS)	(pending)	Risk Matrix TLS Performance-Based

The identified trends have implications for safety assessment. Systems-level changes appear to have increased the scope of analysis. If this trend continues, there will be an increase in the scope of analysis when evaluating expected future systems-level changes. This chapter will describe implications of challenges observed in past case studies to the ability to perform safety assessment and operational approval. One of the key challenges is incorporating increased breadth of safety behavior in the safety assessment process. Increasing demands on safety

assessment quality also result from the increased safety expectations in the system. Implications in assessing fundamentally new operational concepts will also be discussed, as well as limitations in achievable performance due to legacy systems. Identifying these implications is expected to provide an opportunity to improve the ability to achieve future changes.

7.1 Increasing Scope of Analysis Required

An increasing scope of analysis was observed in the cases analyzed. Scope is the number of system elements and hazards/risks evaluated in safety assessment. This trend is illustrated in Figure 7-1. Generally, the trend is for proposed changes to incorporate more system elements and exhibit an increase in interactions with other aircraft and existing systems. The two pending changes reviewed, ADS-B and UAS exhibit large scope compared to previous changes. Trends observed in the scope of analysis are discussed below.

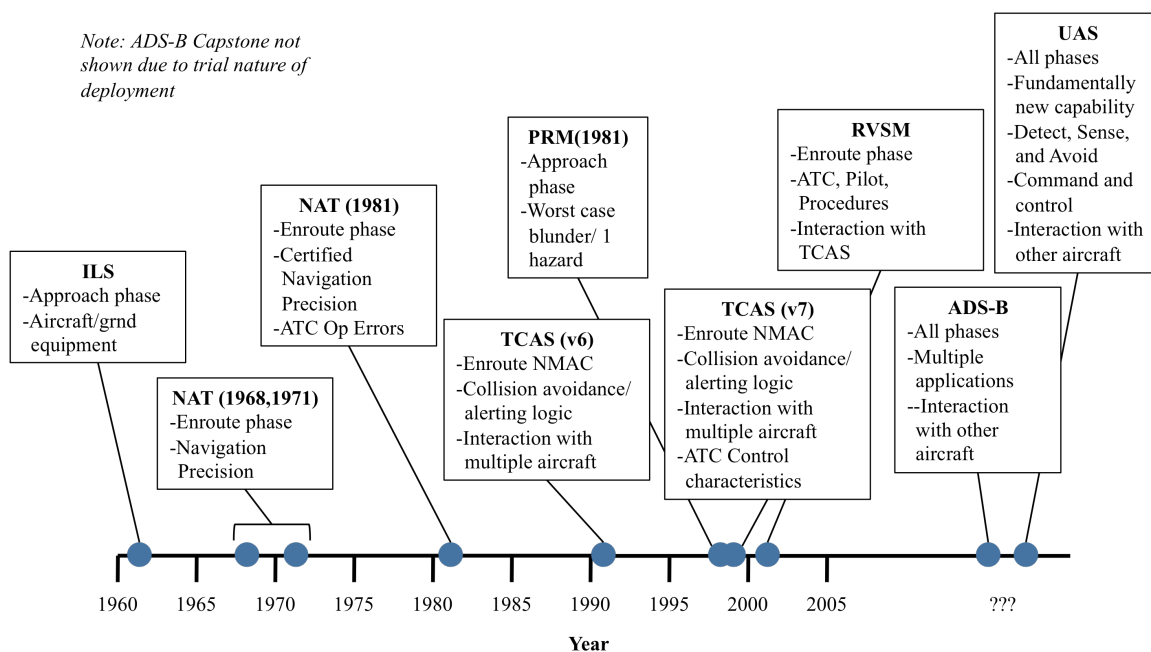


Figure 7-1: Increasing Scope of Reviewed Changes

Distributed functionality is a key property observed in systems-level changes. Multiple components of a system, such as avionics, infrastructure, and procedures interact in performing an operational capability. This is evident in the ADS-B case, where several applications require ground infrastructure, airborne equipment, and procedures. This is also evident for UAS, where

functions are distributed between the unmanned vehicle, ground station, and command and control infrastructure.

Other cases are also large in scale, meaning that there are a large number of elements that compose the change. When this is the case, each element can have multiple failure modes or interactions with other elements. Evaluating the safety performance for a given risk across the multiple system elements that support a function can require a more sophisticated examination of interactions and tradeoffs between system elements. This is one mechanism by which scale increases breadth of scope along the dimension of system elements.

An increase in scale can also be expected to result from the planned implementation of multiple applications reliant upon common infrastructure. With long equipage cycles and time scales of current programs, it will be attractive to support multiple applications associated with changes. Each application has separate risks associated with it and can change the behavior of system elements. Thus, increasing applications expands the scope of risks evaluated. Some consequences in terms of setting required functionality will be discussed in Section 7.5.

One final factor increasing scale is the physical extent of changes to the system. Infrastructure changes can be expected to be deployed across the entire air transportation system. This can create large variation in operating environments, interfaces with automation systems, and interactions with other air traffic of varying levels of capabilities. This increases scope in both the conditions under which the change must be assessed, and interacting with external systems.

7.1.1 Challenges in Managing Complexity of Increased Scope

In past changes, complexity has been managed by decomposing the safety behavior considered by hazard. When a target level of safety method was used, risk was analyzed to a single hazard, and other hazards were scoped out of analysis. This approach relied on a decomposition of influence in the change to define a focused hazard for assessment. Using a risk matrix approach, causal behavior was assessed to individual hazards, and in some cases to groups of hazards. The strategy of decomposition is likely to be less appropriate for future changes due to coupling in behavior and potential adverse consequences due to decomposition.

In the risk matrix approach, risk levels are assessed by decomposing the analysis by hazard. There is also a chance that the decomposition strategy to individual hazards can increase the overall risk levels outside of the scope of analysis if defined mitigations interact to adversely influence the level of other risks. The common strategy to manage this is to implement mitigations that are isolated to the individual risk and not expected to interact, or to introduce mitigations that are expected to enhance safety across a broad set of hazards. This strategy can result in sub-optimal design of mitigations by not evaluating tradeoffs in the performance of mitigation measures across hazards. Thus, assessing each hazard individually can lead to overspecification of requirements in the system, such that multiple mitigations address multiple hazards.

7.1.2 Use of the Influence Matrix to Structure Scope Decisions

The scoping decision is an important process in safety assessment. The process has a strong effect in defining the comprehensiveness of analysis by determining what influences can be expected to contribute significantly to risks, and what influences can be scoped out of the safety assessment. There is currently a lack of structured processes used for defining the scope of safety assessment.

The influence matrix can be used to explicitly address scope decisions made in safety assessment at a systems-level. Population of the influence of system elements on hazards and risks can clearly communicate and document assumptions made about the safety behavior of a system before detailed modeling and analysis are performed.

The influence matrix can also identify potential approaches to decomposing the assessment of safety behavior. This can be achieved by identifying clusters of common influence groupings on risks, which can be used to structure the detailed modeling and analysis processes around groups of risks with common mitigation strategies. This provides the potential to decompose safety assessment tasks while maintaining an increased scope. It also highlights what elements with high influence are considered outside the scope of analysis, and highlights assumptions made about behavior external to analysis.

7.2 Increasing Demands on the Quality of Safety Assessment

The trend of decreasing accident rates can be expected to lead to an increase in required safety performance of changes. This is supported by trends that have been observed in case studies of reductions in the Target Level of Safety. There has also been an observed increase in the sophistication of safety models. With the desire to continue safety improvements recognized by the FAA, increasing demands on the quality of safety assessment can be expected in the future.

7.2.1 Increasing Safety Expectations

As accident rates have decreased, the requirement to maintain safety in proposed changes has resulted in increased safety expectations. This is evident in the trend of decreasing Target Levels of Safety in the cases reviewed, as illustrated in Figure 7-2. Although there are differences in the type of accident, the TLS for PRM performance is two orders of magnitude higher than the TLS for RVSM, and intermediate cases support a generally decreasing trend.

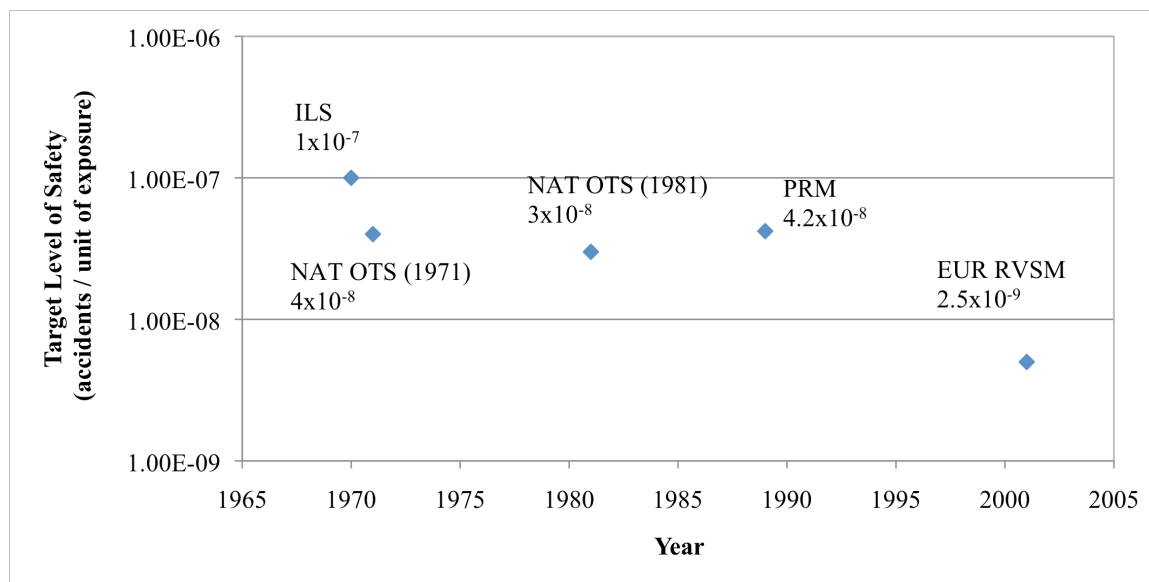


Figure 7-2: Target Levels of Safety from Cases Reviewed

7.2.2 Increasing Accuracy Expected in Safety Assessment

In early application of quantitative risk models, results were used to augment judgment by operational experts and validate assumptions. Over the course of time, as more operational data has become available, and sophistication of modeling and computational tools have increased, safety models have become more representative of operational data. This is evidence of an increase in the expected accuracy of safety assessment.

More sophisticated models often require an increase in representative operational data extrapolated to low probability events, especially in the analysis of midair collision risk. This will present a challenge for future systems-level changes, especially when experience from past operations may not directly transfer to a new capability, as will be discussed in Section 7.3.

Judgment by assessors remains a key factor in assigning probabilities to human failure modes. In the case where human performance results in observable operational errors or incidents, it may be possible to observe historical probabilities to use in safety assessment. However, under new operating conditions, significant operational expertise is required to accurately represent how human elements will interact with the operation of the system under varying conditions and in the presence of potential failure modes.

7.2.3 Increasing Scope Required to Accurately Represent Behavior

Expansion of Hazards Considered. The need to accurately predict expected levels of risk can also be expected to result in an increase in the required scope of safety assessment. As discussed in Section 4.4.3, negligible risks are commonly eliminated from scope when dominant conditions are present. In the risk matrix approach, hazards with low risk levels may be scoped out of the design if they are not expected to substantially affect the overall level of risk of the change. In the TLS approach, this scoping is performed implicitly, assuming that there is not significant influence on other hazards that have been decomposed in the risk budget.

The system typically becomes safer by mitigating dominant risk levels associated with hazards. Hazards with a higher level of risk are more likely to occur in operation, making them more likely to be identified and corrected. This represents a paradox in ultra-reliable systems, as

articulated by Amalberti [99]. The increased safety performance results in less ability to address risks based on accidents.

The need for an expanded scope of analysis can be illustrated by an example using the influence framework, as shown in Figure 7-3. Two hazards influencing a risk are shown. The first hazard has been assigned set of notionally strong influences across several system elements, with a few weak or negligible elements. The level of risk associated with the second hazard is only influenced weakly by changes in one element. This is typically correlated with a very low change in risk level. Under the assumption that other hazards dominate, the second hazard would be scoped out of the analysis. When the scope of analysis expands, addressing an influence, although it is weak, is required to reduce overall risk levels by a significant magnitude.

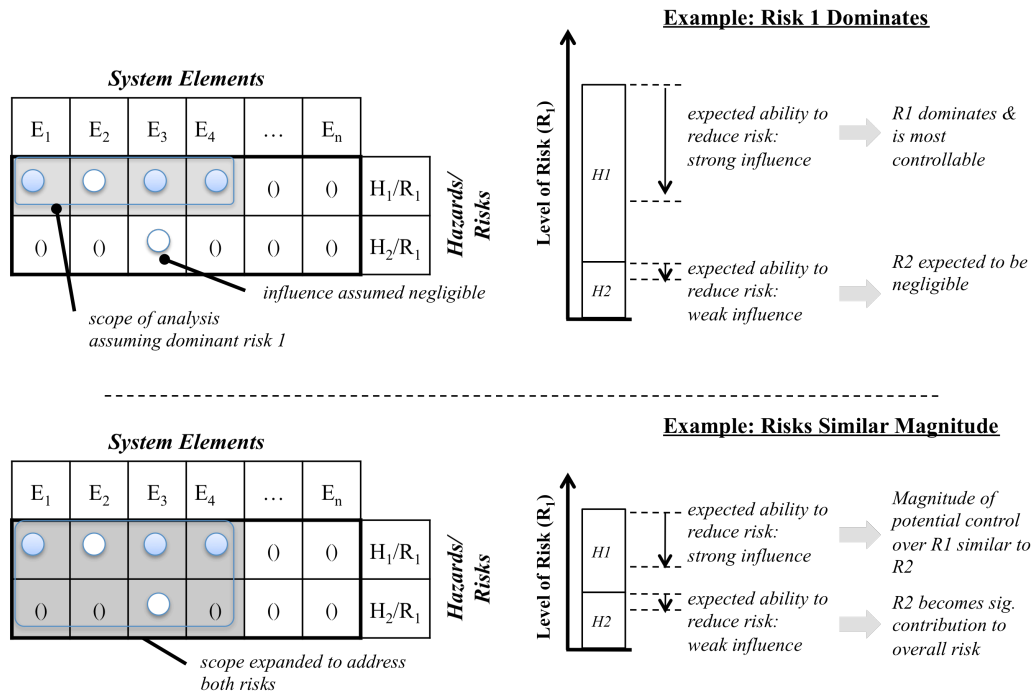


Figure 7-3: Expansion of Scope of Analysis

A reduction in dominant hazards can lead to a significant increase in the number of hazards evaluated. This is illustrated conceptually in Figure 7-4. In the figure, there are multiple hazards shown, each with an associated risk level. The first two hazards have assessed risk levels significantly above the notional acceptability threshold, while the others are near the threshold. For the first two hazards, it is clear that risk needs to be mitigated. For the other hazards, it is

less apparent that risk should be mitigated, or what the most effective mitigation strategies may be. With a reduction in dominant hazards, it will become more difficult to determine effective mitigations.

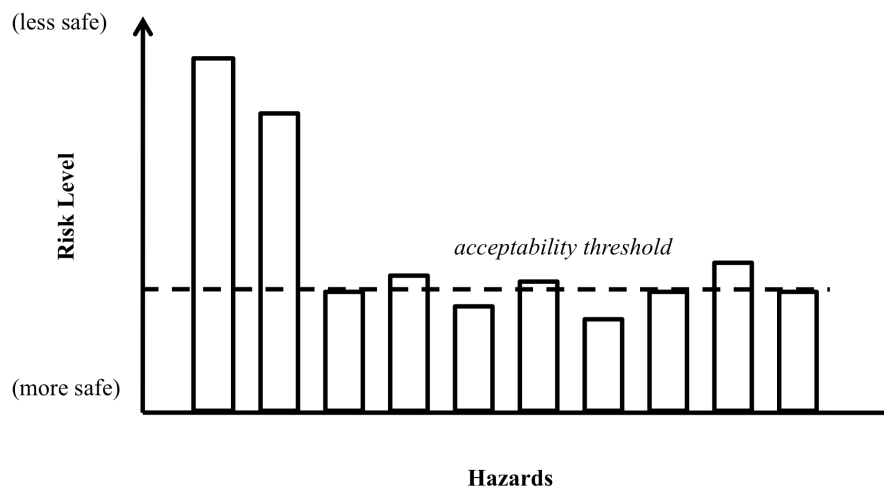


Figure 7-4: Illustration of Consequences of Dominant Hazards

For hazards with risk levels close to acceptability criteria, mitigation strategies can be ambiguous. Without a dominant hazard, there can be a large number of hazards near the acceptability threshold. Mitigating any individual hazard would not substantially reduce risk levels, which are already very low.

It can become more difficult to rationally determine which hazards to mitigate. Each hazard has a cost associated with mitigation to an acceptable level, and with an increase in hazards it can be difficult to determine how to allocate mitigation resources. It may also become more difficult to identify mitigations that do not interact to increase the risk level for other hazards. To address this challenge, there may be a need to develop analysis of mitigations at a meta-level that can affect multiple hazards.

There is also the possibility that if the increased number of hazards cannot be mitigated, acceptable scope may be limited to achieve tractability of analysis. This would limit the types of changes to the system that can be approved.

Dynamic & Emergent Behavior. One result of the expansion of scope can be to further identify more subtle system behavior. Hazards can exhibit complex causal behavior that is difficult to identify in early assessment of systems. The presence of emergent behavior manifest as systems accidents motivates the need to expand the scope of analysis to additional system elements. System accidents typically occur due to the complex interaction of multiple elements [25] and are especially challenging to detect when there is no clear causal failure leading to the accident. Due to increasing system complexity, scope is likely to expand both in addressing interactions with additional external elements and their resultant risks. The goal is to address potential emergent behavior early in the process to prevent that behavior from resulting in an accident.

7.2.4 Use of Operational Monitoring as a Mitigation

Operational monitoring measures can be considered as an approach to mitigation risks in the safety assessment process. While this has been performed for limited examples, it is not part of current safety assessment or operational approval guidance. Including monitoring as a mitigation can be a strategy to approve changes where procedural or technical mitigations were not sufficient to achieve acceptable risk levels at the time. Monitoring can also expand the scope of authority to correct safety deficiencies to external elements.

Appropriate measures must be taken to ensure that monitoring can reduce risk by addressing precursors to accidents before an accident occurs. Monitoring mitigations should not reduce the level of safety of the system.

7.3 Assessment Challenges from Fundamentally New Types of Operations

Many expected systems-level changes exhibit fundamentally new types of operation in the air transportation system. Due to the nature of new types of operation, there is a reduced ability to apply past experience and judgment, operational data, and similarity strategies to evaluation of expected safety behavior.

Lack of Ability to Apply Similarity. The approach of limiting scope by similarity is challenging fundamentally new types of operation, and is likely to not be appropriate. When an operation is significantly different, an analogous operation in the current system does not exist. The scope of

assessment is therefore likely to increase, as additional safety behavior must be evaluated. By a similar argument, the performance-based approach is not appropriate to simplify the assessment of fundamentally new capabilities.

In the case where multiple risks are evaluated and multiple system elements influence the risk, this increase in scope is likely to increase uncertainty in the resultant level of risk of the system. Following the discussion of uncertainty, another cause of increased scope is discussed. Operations may be implicitly accepted today that would not meet current safety assessment criteria. Even in performing similar functionality to the system, they cannot be accepted by similarity due to the unacceptable performance of a reference system.

There is the risk that lack of similarity will fundamentally limit the types of operational capabilities that can be approved. If sufficient uncertainty exists such that the level of risk associated with a new capability cannot be evaluated, the safety case may fail to close and the change could be rejected. It is also possible that performance requirements may be made sufficiently stringent that they are not realizable by the current state of technology.

Need to Obtain Operational Data in Early System Deployments. The representativeness of operational data presents a paradox in safety assessment. Operational data must reflect the expected operational environment, but that environment is unknown unless a reasonably similar system exists in operation. When a proposed change significantly alters the behavior underlying past data, it is difficult to judge the applicability of past experience to the assessment of the proposed change.

It should be recognized that human judgment remains a key factor in extrapolating trends in operational data beyond the likelihood available from samples. This judgment should also be recognized as having an ability to adapt past data to conditions of interest for the current change evaluated. An example of this approach is evident in the case of collision risk assessment of Unmanned Aircraft Systems (UAS). The data limitation is being overcome by modifying past operational data to reflect expected changes in interaction with future UAS systems. Parameters of the encounter model used to evaluate TCAS have been altered to reflect potential conflicts with UAS, which can have different performance from current commercial aircraft [100].

It is a challenge when the operation of a new system is sufficiently different from current operation such that past experience does not apply. In this case, data from early operational implementations can be especially useful. It will therefore be essential to structure programs to identify relevant safety data required in operational trials that can inform the safety assessment for future refinements of the system.

7.4 Limitations in Achievable Performance due to Interaction with Legacy Systems

Proposed changes often interact with elements in the existing system. In some cases, the current structure of operational approval of limits the ability to change the behavior of existing systems. This inability to change the behavior of existing legacy systems can constrain the achievable performance of proposed changes. This has been observed in RVSM and ADS-B.

7.4.1 Performance Limitations of Legacy Systems

In classes of changes that interact significantly with TCAS, achievable separation distances can be limited if these interactions are not mitigated through additional safety requirements in the change. There is also the risk that mitigations may not acceptably reduce risk, and therefore achievable separation will be limited.

The effectiveness of TCAS at mitigating midair collision risk levels may also constrain achievable operational concepts. Where other aircraft are not equipped with transponders, the effect of mitigation is reduced, and midair collision risk may be unacceptable. This class of interactions can therefore limit the physical extent of allowable changes to airspace where equipage is ensured.

A separate challenge due to legacy system performance is illustrated by the requirements on ADS-B navigation quality indicators for mixed environments compared to non-radar environments. Paradoxically, with two available position sensors (ADS-B and radar), higher navigation precision is required for the mixed environment than when relying on only one position source (ADS-B).

7.4.2 High Performance Requirements Set by Lower Performance System Elements

Where there is significant variation in equipage of other aircraft, the lowest performance equipment class can set the performance requirements for an overall application. This is especially relevant for cases where the risk is a midair collision. By its nature, midair collision risk couples behavior between systems through common interaction in airspace.

This challenge is emerging for the case of unmanned aircraft systems. Interaction with non-transponder equipped aircraft creates a significant challenge for the design of Detect Sense and Avoid Systems (DSA). Current approaches to DSA require active rather than passive sensors to detect aircraft that do not emit transponder signals [100]. These sensors replace the active pilot ability to detect, sense, and avoid other objects.

This challenge can arise from not considering airspace design as within the scope of most significant changes. Due to the current mix of operations in certain classes of airspace, it is expected to become increasingly difficult to achieve advanced capabilities without enforcing equipage requirements on other users, or specifying proposed systems to higher levels of performance.

7.5 Balancing Required Performance In Long Time Scales of Change

In several cases, underlying infrastructure is used for a common set of applications. For example, ADS-B supports multiple applications in the current plans for deployment [101]. It is expected to enable additional applications in the future. One challenge present with multiple applications is balancing current and future demands for functionality. This will be discussed in the first section. In the second section, the challenge of requirements stability based on continued revision of definitions of required performance will be addressed.

7.5.1 Future vs. Current Demands for Functionality

Initial applications of a new technology may be implemented at lower criticality [102], meaning that failure modes are generally of less severe consequence. This can occur due to the uncertainty in safety performance of the capability. Failures of functions that are not flight critical can be more readily mitigated through existing controls in the system. Lower criticality

of function also implies a lower level of required software design assurance, and other factors that are more likely to speed initial development.

Lower levels of requirements, even if not directly related to the flight criticality, also reduce the cost of equipage. Requirements on navigation precision that are less demanding tend to be met by existing aircraft infrastructure, while there is the concern that methods such as WAAS or LAAS that provide higher levels of precision are either not fully deployed, or too expensive [103].

With long implementation and equipage times, there will be a challenge in operational approval in the tradeoff between establishing initially low requirements based on expected initial use compared to requiring increased performance for anticipated future applications. This tradeoff is illustrated notionally in Figure 7-5. If the former approach is taken, there is a risk that the system will be specified at point A, and will be underspecified for the higher level of requirements at B. This can potentially require a second equipage cycle, or limit the ability to achieve future functionality. If the latter approach is taken, there is a risk that a system will be overspecified and less attractive to operators for immediate benefits.

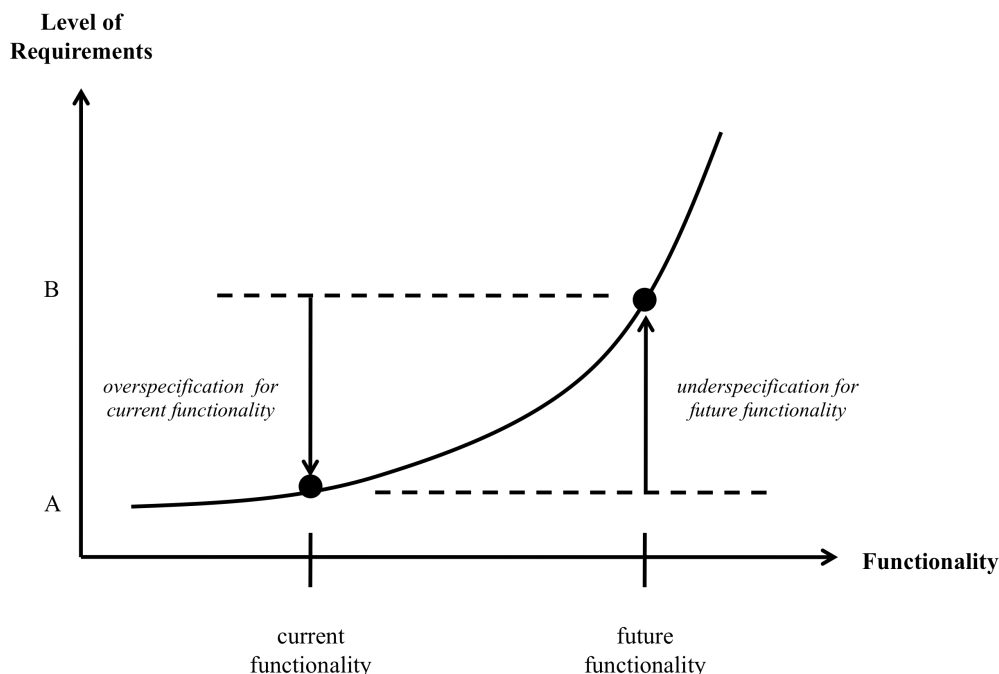


Figure 7-5: Current vs. Future Functionality and Levels of Requirements

7.5.2 Requirements Stability

Long lead times have implications for the stability of underlying requirements [104]. Because standards are developed before operational approval of systems, there is significant uncertainty in potential costs of recertification or reequipping if the avionics installed by early adopters are not adequate to perform desired functions.

Uncertainty in standards can create a disincentive for operators to equip with a technology that meets the current standards if their avionics may not be usable in the future or if revised standards provide a higher level of benefits.

7.6 **Summary**

Systems-level changes have increased in the scope of analysis. If this trend continues, there will be an increase in the scope of behavior assessed when evaluating expected safety performance and implementing required mitigations. There will also be increasing demands for safety performance as accident rates have decreased and as regulators seek to further decrease the level of risks in the system. This is expected to increase demands on the quality of safety assessment to accurately predict adverse behavior.

In addition, future changes are expected to introduce fundamentally new operational capabilities, changing the way that the air transportation system operates. These new capabilities make it less appropriate to apply previous operational experience or build on similarity to past behavior. This can increase demands on safety performance and implicitly introduce additional uncertainty on its results.

In combination, the trends highlighted from pending ADS-B and UAS changes indicate increasing challenges in conducting safety assessment for future systems-level changes. There is a risk that the safety assessment may become intractable, resulting in an inability to realize significant operational improvements in the future.

8 Conclusions and Recommendations for Future Work

Significant challenges can be expected in the safety assessment of the scale of changes envisioned in future modernization initiatives. Along with increasing scale of expected changes, there will also be increasing demands for safety performance resulting in an expanded scope of analysis required. Several other key trends will also present challenges. These include the assessment of fundamentally new types of operation, limitations due to the interface with legacy systems, long time scales of change.

The influence matrix framework presented in this work has been applied to show that the key effect of the identified trends for future safety assessment will be an expansion in the required scope of analysis. There are limits to the achievable scope in safety assessment. Limits can arise from cognitive limits of the assessors in the ability to identify all potential influences of system elements on risk, especially when the interactions of a system are complex. Complex interactions can lead to multiple weak influences, especially through the interaction with external systems and identification of those weak influences can be a limitation for assessors. There can also be resource limitations to the scope of safety assessment in terms of time and effort available to perform the assessment.

If limitations to scope cannot be managed, the system may be constrained to changes for which scope can be managed. This is the foundation for methods of utilizing equivalent functionality. Similar reliance on limited functional changes as a means of reducing the required scope of assessment can limit changes to functionally similar operations.

To accommodate new operational capabilities, limits to scope will need to be overcome. Several approaches may be available to overcome current scoping challenges. To more efficiently perform analysis, it may be possible to develop automated tools to analyze sets of hazards with structured forms of influence. These tools could free assessor resources to focus effort on

hazards where behavior is not understood well enough to be captured in a structured form, thus reducing the scope of assessment performed by human assessors. It should also be possible to reuse results from previous safety assessments where the functions performed by systems are similar. Those hazards that can be reused would also limit the scope of new analysis performed.

Cognitive limitations of assessors can also be overcome through several strategies. Decomposing analysis within areas of expertise is commonly applied, but may only be appropriate for limited hazards where the influence is grouped around common domains, such as aircraft systems, or ATC systems. Automation tools may also be applied to safety assessment to structure the analysis of hazards and influences, to allow for more efficient and common mental models of safety behavior.

There are several challenges in determining the appropriate scope of analysis. If analysis is underscoped, there is an influence of system elements, or additional hazards that can increase cause implemented risk levels to be higher than acceptable. If analysis is overscoped, the additional mitigations imposed upon the system, or additional resources spent on safety assessment are inefficient. The resources associated with the tasks could better be applied to addressing other areas of safety.

Underscoping can have a strong effect on the validity of assessed safety if influences scoped out of analysis significantly increase the level of risk above acceptable values. For this reason, particular attention must be paid to influences on hazards with risk levels near acceptability thresholds. Techniques can be applied that consider potential interactions with additional system elements that may contribute to risk levels for these hazards.

Overscoping can result from current approaches that assess and mitigate risk levels by hazard. If mitigations reduce expected risk significantly below acceptability levels, an excess amount of resources have been expended in the system to implement the mitigations. This results in an increase in the time, cost, and complexity of implementing systems. A potential approach to improve the design of mitigations would be to reassess proposed changes with all mitigations identified to eliminate unnecessary mitigations.

The ability to achieve the appropriate scope of analysis will be key to realizing future changes in the air transportation system. Methods should be developed to enhance the ability to manage increased scope in safety assessment and to achieve the appropriate balance between underscoping and overscoping.

9 Bibliography

- [1] Joint Planning and Development Office, "Next Generation Air Transportation System Integrated Work Plan: A Functional Outline," Version 1.0, September 30 2008, <http://www.jpdo.gov/iwp.asp>, Accessed: June 20, 2009.
- [2] SESAR Consortium, "SESAR Master Plan," March 2009, <http://www.eurocontrol.int/sesar/gallery/content/public/docs/European%20ATM%20Master%20Plan.pdf>, Accessed: June 28, 2009.
- [3] Joint Planning and Development Office, "Enterprise Architecture v2.0 for the Next Generation Air Transportation System," June 22 2007.
- [4] Joint Planning and Development Office, "A comparative assessment of the NextGen and SESAR operational concepts," JPDO Paper 08-001, May 22 2008.
- [5] National Transportation Safety Board, "Aviation Accident Statistics for 2008 Show 'Mixed Picture'," April 2, 2009, <http://www.ntsb.gov/Pressrel/2009/090402b.html>, Accessed: May 4 2009.
- [6] Boeing Commercial Airplanes, "Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations 1959-2008," Seattle, WA, July 2009, <http://www.boeing.com/news/techissues/pdf/statsum.pdf>, Accessed: July 30, 2009.
- [7] Federal Aviation Administration, "Aviation Safety Fiscal Year 2008 Business Plan," December 7 2007, http://www.faa.gov/about/plans_reports/media/AVS%20Business%20Plan%20with%20Cover.pdf, Accessed: April 11, 2008.
- [8] International Civil Aviation Organization, "Manual on Airspace Planning Methodology for the Determination of Separation Minima," Doc 9689-AN/953, 1998.
- [9] B. Glaser and A. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, 11 ed.: Aldine, 1980.
- [10] N. G. Leveson, *System Safety Engineering: Back To The Future*: Massachusetts Institute of Technology, *Unpublished Manuscript*, 2002.
- [11] Federal Aviation Administration, "Federal Aviation Administration Safety Management System Manual," Version 1.2, 2004, http://consolidation.natca.net/SMOperationsTraining/FAA_SMS_Manual-Version_1.1.pdf, Accessed: May 15, 2008.
- [12] CAST/ICAO, "CAST/ICAO Common Taxonomy Team," 2009, <http://www.intlaviationstandards.org/>, Accessed: March 8, 2009.
- [13] Federal Aviation Administration, "FAA System Safety Handbook," December 30 2000, http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/, Accessed: April 2, 2008.
- [14] Department of Defense, "Standard Practice for System Safety," MIL-STD-882D, February 10 2000.

- [15] A. Klinke and O. Renn, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies," *Risk Analysis*, vol. 22, is. 6, pp. 1071-1094, 2002.
- [16] P. Thompson and W. Dean, "Competing conceptions of risk," *Risk: Health, Safety & Environment*, vol. 7, p. 361, 1996.
- [17] C. Starr and C. Whipple, "Risks of Risk Decisions," *Science*, vol. 208, is. 4448, pp. 1114-1119, June 6 1980.
- [18] P. Slovic, *The Perception of Risk*: Earthscan Publications Ltd., 2000.
- [19] P. Slovic, et al., "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality," *Risk Analysis*, vol. 24, is. 2, 2004.
- [20] R. E. Kasperson, et al., "Stigma and the Social Amplification of Risk: Toward a Framework of Analysis" in *Risk, Media and Stigma: Understanding Public Challenges to Science and Technology*, 1st edition., J. Flynn, P. Slovic and H. Kurnreuther ed., London, United Kingdom: Earthscan Publications Ltd., pp. 9-27, 2001.
- [21] R. W. Cobb and D. M. Primo, *The Plane Truth: Airline Crashes, the Media, and Transportation Policy*. Washington, DC: The Brookings Institution, 2001.
- [22] R. W. Cobb and D. M. Primo, *The Plane Truth: Airline Crashes, the Media, and Transportation Policy*: Brookings Institution Press, 2003.
- [23] B. Fischhoff, et al., *Acceptable risk*: Cambridge Univ Pr, 1984.
- [24] J. Rasmussen, "Risk management in a dynamic society: a modeling problem," *Safety Science*, vol. 27, is. 2-3, pp. 183-213, 1997.
- [25] C. Perrow, *Normal Accidents: Living with High-risk Technologies*: Princeton University Press, 1999.
- [26] J. Reason, *Managing the Risks of Organizational Accidents*: Ashgate Publishing, 1997.
- [27] J. A. Rijpma, "Complexity, Tight-Coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory," *Journal of Contingencies and Crisis Management*, vol. 5, is. 1, pp. 15-45, March 1997.
- [28] E. Hollnagel, et al., *Resilience engineering: Concepts and precepts*: Ashgate Publishing, Ltd., 2006.
- [29] International Civil Aviation Organization, "Safety Management Manual (SMM)," 2006, http://www.icao.int/fsix/Library/SMM-9859_1ed_en.pdf, Accessed: April 6, 2008.
- [30] RTCA Inc, "Guidelines for the Approval of the Provision and Use of Air Traffic Services Supported by Data Communications," RTCA/DO-264, December 14 2000.
- [31] SAE, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," ARP 4761, December 1 1996.
- [32] F. Netjasov and M. Janic, "A review of research on risk and safety modelling in civil aviation," *Journal of Air Transport Management*, vol. 14, is. 4, pp. 213-220, 2008.
- [33] N. Leveson, "A new accident model for engineering safer systems," *Safety Science*, vol. 42, is. 4, pp. 237-270, April 2004.
- [34] K. Marais, "A New Approach to Risk Analysis with a Focus on Organizational Risk Factors," Ph.D. Dissertation, *Department of Aeronautics & Astronautics, Massachusetts Institute of Technology, Cambridge, MA*, June 2005.
- [35] H. A. P. Blom, et al., "Accident risk assessment for advanced ATM" in *Air Transportation Systems Engineering*, G. L. Donohue and A. G. Zellweger ed.: American Institute of Aeronautics and Astronautics, pp. 463-480, 2001.

- [36] J. Luxhoj, "Risk analysis of human performance in aviation maintenance," in *Proceedings of the 16th human factors in aviation maintenance symposium (HFIAM 2002)*, San Francisco, California, 2002.
- [37] P. Bishop, et al., "A Methodology for Safety Case Development," *Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham 1998*, pp. 194-203, 1998.
- [38] D. Jackson, et al., *Software for Dependable Systems: Sufficient Evidence?* Washington, DC: National Academies Press, 2007.
- [39] RTCA Inc, "Software Considerations in Airborne Systems and Equipment Certification," RTCA/DO-178B, December 1 1992.
- [40] A. Mozdzanowska, "System Transition: Dynamics of Change in the US Air Transportation System," Doctor of Philosophy, *Engineering Systems Division, Massachusetts Institute of Technology, Cambridge, MA*, 2008.
- [41] K. Marais and A. Weigel, "Encouraging and ensuring successful technology transition in civil aviation," March 2006, <http://esd.mit.edu/WPS/esd-wp-2006-07.pdf>, Accessed: May 5, 2009.
- [42] RTCA Inc, RTCA, Inc, "Final Report of the RTCA Task Force 4, Certification," Washington, DC, February 26 1999.
- [43] United States Government Accountability Office, "Air Traffic Control - FAA Needs to Ensure Better Coordination When Approving Air Traffic Control Services," Washington, DC, November 2004, <http://www.gao.gov/new.items/d05111.pdf>, Accessed: April 6, 2008.
- [44] D. Robyn, The Brookings Institution, "Air Support: Creating a Safer and More Reliable Air Traffic Control System," Washington, DC, July 2008.
- [45] United States General Accounting Office, "National Airspace System - Persistent Problems in FAA's New Navigation System Highlight Need for Periodic Reevaluation," Washington, DC, June 2000 <http://www.gao.gov/new.items/r100130.pdf>, Accessed: April 6, 2008.
- [46] M. Hansen, et al., "Understanding and Evaluating the Federal Aviation Administration Safety Oversight System," July 2006, <http://www.nextor.org/pubs/NR-2006-001.pdf>, Accessed: September 19, 2008.
- [47] DOT Office of the Inspector General, "FAA Is Not Realizing the Full Benefits of the Aviation Safety Action Program," AV-2009-057, May 19 2009.
- [48] J. Downer, *Burden of Proof: Regulating Ultra-High Reliability in Civil Aviation*, Unpublished Manuscript, 2006.
- [49] T. Ross, "Accurate confidence intervals for binomial proportion and Poisson rate estimation," *Computers in biology and medicine*, vol. 33, is. 6, pp. 509-531, 2003.
- [50] D. Fowler, et al., "So It's Reliable But Is It Safe? A More Balanced Approach to ATM Safety Assessment," in *7th USA/Europe ATM 2007 R&D Seminar, July 2-5, Barcelona, Spain*, 2007.
- [51] P. Brooker, "Air traffic safety: Continued evolution or a new paradigm?," *Aeronautical Journal*, vol. 112, is. 1132, pp. 333-344, 2008.
- [52] D. Fowler, et al., "2020 Foresight: A systems-engineering approach to assessing the safety of the SESAR Operational Concept " *Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM2009)*, Napa, California, June 2009.
- [53] "Definitions and Abbreviations," *CFR 14 Part 1*, January 15, 2009.

- [54] Federal Aviation Administration, "Safety Risk Management Guidance For System Acquisitions, Edition 1.4," ATO-S 2006-1, December 21 2006, http://fast.faa.gov/toolsets/Safmgmt/docs/SRMGSA_1.4a.pdf, Accessed: April 3, 2008.
- [55] Eurocontrol, "Eurocontrol Safety Regulatory Requirement 4 - Risk Assessment and Mitigation in ATM," May 4 2001.
- [56] L. A. Cox, "What's Wrong with Risk Matrices?," *Risk Analysis*, vol. 28, is. 2, pp. 497-512, 2008.
- [57] Federal Aviation Administration, "Equipment, Systems, and Installations in Part 23 Airplanes," Advisory Circular AC 23.1309-1C, March 12 1999.
- [58] Federal Aviation Administration, "System Design and Analysis," Advisory Circular AC 25.1309-1A, June 21 1988.
- [59] Federal Aviation Administration, "Type Certification," Order 8110.4C, Change 1, March 28 2007.
- [60] Federal Aviation Administration, "Airworthiness Certification of Aircraft and Related Products," Order 8130.2F, Change 3, April 18 2007.
- [61] "Ultralight Vehicles," *CFR 14 Part 103*, August 18, 2008.
- [62] Federal Aviation Administration, "Production Approval and Certificate Management Procedures," Order January 30 2009.
- [63] Federal Aviation Administration, "Parts Manufacturer Approval Procedures," Order 8110.42C, June 23 2008.
- [64] "Certification Procedures for Products and Parts," *CFR 14 Part 21*, August 18, 2008.
- [65] Federal Aviation Administration, "Technical Standard Order Program," Order 8150.1B, May 12 2002.
- [66] J. M. Histon, "Mitigating Complexity in Air Traffic Control: The Role of Structure-Based Abstractions," Ph.D., *Department of Aeronautics & Astronautics, Massachusetts Institute of Technology, Cambridge, MA*, June 2008.
- [67] Federal Aviation Administration, "AOV Credentialing and Control Tower Operator Certification Programs," Order 8000.90, August 11 2006.
- [68] Federal Aviation Administration, "Airway Facilities Maintenance Personnel Certification Program," Order 3400.3H, March 5 2002.
- [69] Federal Aviation Administration, "General Technical Administration" in *Flight Standards Information Management System (FSIMS)*, 2007.
- [70] Federal Aviation Administration, "United States Standard for Terminal Instrument Procedures (TERPS)," Order 8260.3B, December 7 2007.
- [71] Federal Aviation Administration, "Flight Procedures and Airspace," Order 8260.19D, August 27 2007.
- [72] "IFR Altitudes," *CFR 14 Part 95*, August 20, 2008.
- [73] Federal Aviation Administration, "Configuration Management Policy," Order 1800.66 Change 2, September 19 2007.
- [74] Federal Aviation Administration, "NAS Architecture 6," August 6, 2008 2008, <http://nas-architecture.faa.gov/nas/home.cfm>, Accessed: August 15 2008.
- [75] Federal Aviation Administration, "NAS Change Proposal (NCP) Process Support of the Safety Management System," Notice N JO 1800.2, September 28 2006.
- [76] Federal Aviation Administration, "FAST - The Federal Aviation Administration Acquisition System Toolset," April 2008 2008, <http://fast.faa.gov/>, Accessed: June 2 2008.

- [77] V. Hilderman and T. Baghai, *Avionics Certification: A Complete Guide to DO-178 (Software), DO-254 (Hardware)*: Avionics Communications, Inc, 2007.
- [78] RTCA Inc, "Design Assurance Guidance for Airborne Electronic Hardware," DO-254 / ED-80, April 2000.
- [79] Federal Aviation Administration, "RTCA, Inc., Document RTCA/DO-178B," Advisory Circular AC 20-115B, January 11 1993.
- [80] Federal Aviation Administration, "RTCA, Inc. Document RTCA/DO-254, Design Assurance Guidance for Airborne Electronic Hardware," AC 20-152, June 30 2005.
- [81] Federal Aviation Administration, "FY 2009 1st Quarter Performance Report," January 30 2009, http://www.faa.gov/about/plans_reports/Performance/quarter_scorecard/, Accessed: April 19 2009.
- [82] Federal Aviation Administration, "ASIAS Home," 2009, <http://www.asias.faa.gov>, Accessed: April 19 2009.
- [83] National Transportation Safety Board, "Special Investigation Report on Emergency Medical Services Operations," Washington, DC., 2006.
- [84] AOPA Air Safety Foundation, "2007 Nall Report - Accident Trends and Factors for 2006," 2007.
- [85] Department of Transportation, "The Department of Transportation's Rulemaking Process," MH-2000-109 July 20 2000.
- [86] United States General Accounting Office, "Aviation Rulemaking - Incomplete Implementation Impaired FAA's Reform Efforts," Testimony GAO-01-950T, July 11 2001, <http://ntl.bts.gov/lib/11000/11200/11288/d01950t.pdf>, Accessed: April 19, 2009.
- [87] N. G. Leveson, *Safeware: System Safety and Computers*: Addison-Wesley, 1995.
- [88] W. E. Vesely, et al., U.S. Nuclear Regulatory Commission, "Fault Tree Handbook," NUREG-0492, January 1981, <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/>, Accessed: June 22, 2009.
- [89] N. Y. Mineta, "Avoiding Aviation Gridlock and Reducing the Accident Rate," December 1997, <http://www.faa.gov/NCARC/reports/pepele.htm>, Accessed: September/28/2008.
- [90] R. E. Machol, "An Aircraft Collision Model," *Management Science*, vol. 21, is. 10, pp. 1089-1101, June 1975.
- [91] ICAO, "Manual on Implementation of a 300m (1000ft) Vertical Separation minimum Between FL290 and FL410 Inclusive," Document 9574, 1990.
- [92] B. Tiemeyer, Eurocontrol, "EUR RVSM Programme, Functional Hazard Assessment," RVSM 697, Version 1.0, February 2001, <http://www.ecacnav.com/downloads/RVSM%20FHA%20V10%2012FEB2001.pdf>, Accessed: February 4, 2009.
- [93] P. Brooker, "Aircraft Collision Risk in the North Atlantic Region," *Journal of the Operational Research Society*, vol. 35, is. 8, pp. 695-703, 1984.
- [94] Eurocontrol, "The EUR RVSM Pre-Implementation Safety Case," Version 2.0, 14 August 2001.
- [95] Eurocontrol, "The EUR RVSM Post-Implementation Safety Case," RVSM A1190, July 28 2004, http://www.ecacnav.com/downloads/EUR%20RVSM%20POSC%20V2.0%2028July%202004_ch_acc.pdf, Accessed: April 12, 2008.
- [96] P. Brooker, "Consistent and Up-to-Date Aviation Safety Targets," *Aeronautical Journal*, vol. 108, is. 1085, July 2004.

- [97] M. I. Izquierdo, Eurocontrol, "The EUR RVSM Safety Monitoring Report 2004," AFN-NAV-PER-SAF-001-2004, 2004, <http://www.ecacnav.com/downloads/AFN-NAV-PER-SAF-001-2004-v02-15-nov.pdf>, Accessed: May 2, 2009.
- [98] D. Fowler, "EUR RVSM POSC Development - FHA Review Report," S.P1193.12.5, January 3 2003, <http://www.ecacnav.com/downloads/FHA%20Report%20V10%20Final.pdf>, Accessed: April 12, 2008.
- [99] R. Amalberti, "The paradoxes of almost totally safe transportation systems," *Safety Science*, vol. 37, is. 2-3, pp. 109-126, 2001.
- [100] J. Kuchar, et al., "A Safety Analysis Process for the Traffic Alert and Collision Avoidance System (TCAS) and See-and-Avoid Systems on Remotely Piloted Vehicles," *AIAA 3rd Unmanned Unlimited Technical Conference*, Chicago, IL2004.
- [101] Federal Aviation Administration, "National Airspace System Architecture 6, Automatic Dependent Surveillance, Broadcast," June 2 2009, http://nas-architecture.faa.gov/nas/prog/program/program_data.cfm?prog_id=281&&CFID=8211248&CFTOKEN=86191bfc2a8e90a4-36A4D4E9-5056-853D-B0D6AAD2DE547150, Accessed: June 5, 2009.
- [102] "Interview," Personal to M. Castle, April 25 2007.
- [103] "Report from the ADS-B Aviation Rulemaking Committee to the Federal Aviation Administration," FAA-2007-29305-0221.1, September 26 2008.
- [104] A. Mozdzanowska, et al., "Feedback model of air transportation system change: Implementation challenges for aviation information systems," *Proceedings of the IEEE*, vol. 96, is. 12, pp. 1976-1991, 2008.
- [105] R. W. Howard, "Progress in the Use of Automatic Flight Controls in Safety-Critical Applications," *The Aeronautical Journal*, vol. 84, October 1980.
- [106] R. Cherry, "The probabilistic approach to safety - success or failure?," *Proc Instn Mech Engrs*, vol. 209, is. 3, pp. 177-184, 1995.
- [107] R. E. Machol, "Thirty Years of Modeling Midair Collisions," *Interfaces*, vol. 25, is. 5, pp. 151-172, September-October 1995.
- [108] B. L. Marks, Royal Aircraft Establishment, Farnborough, United Kingdom, "Air Traffic Control Separation Standards and Collision Risk," RAE Tech Note No. Math 91, 1963.
- [109] P. G. Reich, "Analysis of long-range air traffic systems: Separation standards - I," *Journal of Navigation*, vol. 19, is. 1, pp. 88-96, 1966.
- [110] E. H. Davies and A. G. Sharpe, NATS U.K., "Review of the Target Level of Safety for NAT MNPS Airspace," London, CS Report 9301, 1999.
- [111] P. G. Reich, "Analysis of long-range air traffic systems. Pt. 1: separation standards (with comments from Stanley Ratcliffe)," *Journal of Navigation*, vol. 50, is. 3, pp. 436-47, 1997.
- [112] International Civil Aviation Organization, "The Introduction of a Reduced Lateral Separation into the NAT Airspace" in *Manual on Airspace Planning Methodology for the Determination of Separation Minima*, 1st edition., 1998.
- [113] Federal Aviation Administration, "Introduction to TCAS II Version 7," November 2000, http://www.sisadminov.net/tcas/docs/TCAS_II_V7.pdf, Accessed: April 19, 2009.
- [114] J. Lebron, US Dept. of Transportation, Federal Aviation Administration, "System safety study of minimum TCAS II," DOT/FAA/PM-83/36, MTR-83W241, 1984.
- [115] K. Carpenter, QinetiQ, "ACAS Safety Studies," February 4 2004, http://www.eurocontrol.int/msa/gallery/content/public/documents/ACAS_safety_studies.pdf, Accessed: July 1, 2009.

- [116] ICAO, "Historical and Future Role of the Airborne Collision Avoidance System (ACAS)," AN-Conf/11-IP/7, October 3 2003, http://www.icao.int/icao/en/anb/meetings/anconf11/documentation/ANConf11_ip007_en.pdf, Accessed: July 1, 2009.
- [117] A. C. Drumm, MIT Lincoln Laboratory, "Lincoln Laboratory Evaluation of TCAS II Logic Version 6.04a," ATC-240, February 21 1996.
- [118] B. J. Chludzinski, MIT Lincoln Laboratory, "Lincoln Laboratory Evaluation of TCAS II Logic Version 7," ATC-268, December 13 1999.
- [119] C. Johnson, "Final report: review of the BFU Uberlingen accident report, version 1: 17/12/2004," *contract C/I.369/HQ/SS/04. Technical report, EUROCONTROL*, 2004.
- [120] J. K. Kuchar and A. C. Drumm, "The Traffic Alert and Collision Avoidance System," *Lincoln Laboratory Journal*, vol. 16, is. 2, pp. 277-296, s 2007.
- [121] Eurocontrol, "Eurocontrol - TCAS II version 7.1," June 26 2009, http://www.eurocontrol.int/msa/public/standard_page/ACAS_Upcoming_Changes.html, Accessed: July 1 2009.
- [122] Eurocontrol, "FARADS (Feasibility of ACAS RA Downlink Study) Close-out Report," 07/05/31-25, 2007.
- [123] J. Andrews, et al., "Safety analysis for advanced separation concepts," *Air Traffic Control Quarterly*, vol. 14, is. 1, pp. 5-24, 2006.
- [124] Federal Aviation Administration, "Precision Runway Monitor Demonstration Report," DOT/FAA/RD-91/5, February 1991, <http://www.tc.faa.gov/acb300/techreports/RD-91-5.pdf>, Accessed: June 17, 2008.
- [125] A. Lind, Massachusetts Institute of Technology Lincoln Laboratory, "Two simulation studies of precision runway monitoring of independent approaches to closely spaced parallel runways," DOT/FAA/NR-92/9, March 2 1993, http://www.ll.mit.edu/mission/aviation/publications/publication-files/atc-reports/Lind_1993_ATC-190_WW-15318.pdf, Accessed: July 3, 2009.
- [126] Federal Aviation Administration, "Separation Standards Working Group Final Report," September 20 2006.
- [127] S. Agoaka and O. Amai, "Estimation accuracy of close approach probability for establishing a radar separation minimum," *The Journal of Navigaton*, vol. 44, pp. 110-121, January 1991.
- [128] JAA, "Guidance Material on the Approval of Aircraft and Operators for Flight in Airspace above Flight Level 290 Where a 300M (1,000 ft) Vertical Separation Minimum is Applied," Leaflet No 6, Revision 1, January 10 1999, <http://www.ecacnav.com/downloads/TGL6rev1.pdf>, Accessed: June 14, 2009.
- [129] J. Scardina, "Overview of the FAA ADS-B Link Decision," June 7 2002, <http://www.icao.int/anb/panels/acp/wg/m/M5wp/Wgm5wp/WGM510.pdf>, Accessed: March 3, 2009.
- [130] Federal Aviation Administration, "Capstone Safety Engineering Report #1 ADS-B Radar-Like Services," December 2 2000, http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/enroute/surveillance_broadcast/wsa/media/SERVOL1.PDF, Accessed: March 2, 2009.
- [131] Federal Aviation Administration, "Surveillance and Broadcast Services Program Segment 1, Safety Risk Management Document: Preliminary Hazard Analysis," SBS-SRMD-062606-1, September 18 2006, http://adsb.tc.faa.gov/WG4_Meetings/ASSAP_MOPS/Mtg09-telecon-2006-1211/ASSAP-WP09-

- 07_SBS%20SRMD%20PHA%20v1%20as%20of%209-18-06.pdf, Accessed: July 5, 2009.
- [132] Federal Aviation Administration and Eurocontrol, "ACTION PLAN 23: Long term ADS-B and ASAS Applications," Draft AP23-08-D4-v0 2, 2008.
 - [133] RTCA Inc., "Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar-Airspace (NRA) Application," RTCA/DO-3-3, December 13 2006.
 - [134] RTCA Inc, "Minimum Aviation System Performance Standards for Aircraft Surveillance Applications," DO-289, December 9 2003.
 - [135] S. D. Thompson and K. A. Sinclair, "Automatic Dependent Surveillance-Broadcast in the Gulf of Mexico," *Lincoln Laboratory Journal*, vol. 17, is. 2, 2008.
 - [136] Federal Aviation Administration, "Request for Approval of a 5NM ADS-B to ADS-B and ADS-B to Radar Separation Standard in the Anchorage FIR," Memorandum, February 9 2007.
 - [137] Federal Aviation Administration, "Resubmittal of Request for Approval of a 5NM ADS-B to Radar Separation Standard in the Anchorage FIR," Memorandum, April 30 2007.
 - [138] European Aviation Safety Agency, "Certification Considerations for the Enhanced ATS in Non-Radar Areas using ADS-B Surveillance (ADS-B-NRA) Application," *AMC 20-24*.
 - [139] RTCA Inc, "Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar-Airspace (NRA) Application," RTCA/DO-303, December 13 2006.
 - [140] U. S. FAA, "ADS-B Out Performance Requirements to Support ATC," Notice of Proposed Rulemaking FAA-2007-29305, 2007.
 - [141] S. Thompson, Staff Member, MIT Lincoln Laboratory, Interview, Conducted: May 11 2007.
 - [142] RTCA Inc, "Minimum Operational Performance Standards for 1090 MHz Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services (TIS-B)," September 13 2000.
 - [143] G. Dunstone, Australian Strategic Air Traffic management Group, ADS-B Implementation Team, "Consideration of Existing ADS-B Avionics," http://www.astra.aero/downloads/ABIT/ABIT-10_IP-007_Existing_Avionics.pdf, Accessed: August 30, 2007.
 - [144] R. Weibel, "Safety Considerations for Operation of Unmanned Aerial Vehicles in the National Airspace System," S.M., *Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, MA*, 2005.
 - [145] K. Dalamagkidis, et al., "Unmanned Aircraft Systems Regulation" in *On Integrating Unmanned Aircraft Systems into the National Airspace System: Issues, Challenges, Operational Restrictions, Certification, and Recommendations*: Springer, pp. 43-62, 2008.
 - [146] Federal Aviation Administration, "Interim Operational Approval Guidance," Policy 08-01, March 13 2008.
 - [147] Federal Aviation Administration, "Right-of-way rules: Except water operations.," *14 C.F.R. 91.113*.
 - [148] ASTM International, "Standard Specification for Design and Performance of an Airborne Sense-and-Avoid System," F2411-04, 2004.
 - [149] R. Schaeffer, "A Standards-Based Approach to Sense-and-Avoid Technology," *ALAA*, vol. 6420, pp. 20-23, 2004.

- [150] RTCA Inc, "Terms of Reference, Special Committee 203, Minimum Performance Standards for Unmanned Aircraft Systems and Unmanned Aircraft," December 16 2005, http://www.rtca.org/CMS_DOC/PMC%20approved%20SC-203%20TOR%20Dec%2016,%202005.PDF, Accessed: October 6, 2008.
- [151] M. Johnson, "Important SC-203 Information for Plenary 10," Personal Communication, E-mail to RTCA Special Committee 203, June 1 2007.
- [152] U.S. House of Representatives, "Unmanned Aerial Vehicles and the National Airspace System," *Transportation and Infrastructure Committee, Aviation Subcommittee*, Washington, DC, March 29 2006.
- [153] K. Hayhurst, et al., National Aeronautics and Space Administration, Langley Research Center, Hampton, Virginia, "Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems," NASA/TM-2007-214539, 2007, <http://shemesh.larc.nasa.gov/people/jmm/NASA-2007-tm214539.pdf>, Accessed: July 2, 2009.
- [154] J. McCarley and C. Wickens, Institute of Aviation, University of Illinois, "Human Factors Concerns in UAV Flight," 2004, <http://www.hf.faa.gov/docs/508/docs/uavFY04Planrpt.pdf>, Accessed: June 2, 2009.

Appendix A

Acronyms & Abbreviations

<i>Acronym</i>	<i>Definition</i>
1090ES	1090 Mhz Extended Squitter
AC	Advisory Circular
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance, Broadcast
AFS	FAA Flight Standards
AIR	FAA Aircraft Certification Service
AMS	Acquisition Management System
ANSP	Air Navigation Service Provider
AOP	Aircraft Owners and Pilots Association
ARC	Aviation Rulemaking Committee
ASIAS	Aviation Safety Information Analysis and Sharing System
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	FAA Air Traffic Organization
ATO-S	FAA ATO Safety Service
ATOS	Air Transportation Oversight System
ATS	Air Traffic Services
COA	Certificate of Authorization
CCB	Configuration Control Board
CM	Configuration Management
CNSRM	Casefile/NCP Safety Risk Management
CRA	Collision Risk Assessment
CRM	Collision Risk Modeling
DAL	Design Assurance Level
DER	Designated Engineering Representative
DSA	Detect, Sense, and Avoid
EUR	[ICAO-designated] European Region
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FHA	Fault (or Failure) Hazard Analysis
FIS-B	Flight Information Services - Broadcast
FL	Flight level
GA	General Aviation
GPS	Global Positioning System
GSN	Goal Structuring Notation

IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
JRC	Joint Resources Council
LAAS	Local Area Augmentation System
LPV	Lateral Precision, Vertical Guidance
MASPS	Minimum Aviation System Performance Standards
MNPS	Minimum Navigation Performance Specification
MOPS	Minimum Operational Performance Standards
NAC	Navigation Accuracy Category
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NAT	[ICAO-designated] North Atlantic Region
NCP	NAS Change Proposal
NIC	Navigation Uncertainty Category
NMAC	Near Midair Collision
NPRM	Notice of Proposed Rulemaking
NTSB	National Transportation Safety Board
NTZ	No Transgression Zone
OTS	Organized Track System (in Oceanic Control)
PMA	Part Manufacturer Approval
PRM	Precision Runway Monitor
RCGSP	[ICAO] Review of the General Concept of Separation Panel
RNP	Required Navigation Performance
RVSM	Reduced Vertical Separation Minima
SA	Selective Availability
SARP	Standard and Recommended Practice
SICASP	[ICAO] SSR Improvements and Collision Avoidance Systems Panel
SIL	Surveillance Integrity Level
SMS	Safety Management System
SPR	Safety and Performance Requirements [Standard]
SRM	Safety Risk Management
SRMD	Safety Risk Management Document
SRMDM	Safety Risk Management Decision Memo
STC	Supplemental Type Certificate
TIS-B	Traffic Information Services - Broadcast
UAS	Unmanned Aircraft System
UAT	Universal Access Transceiver
TCAS	Traffic Alert and Collision Avoidance System
TERPS	United States Standard for Terminal Instrument Procedures
TSO	Technical Standard Order
VDRP	Voluntary Disclosure Reporting Program
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions
WAAS	Wide Area Augmentation System

Appendix B

Documentation of Current Safety Regulatory Processes Reviewed

Agency	Type	Number	Title
DoD	Standard	MIL-STD-882D	Standard Practice for System Safety
Eurocontrol	Regulatory Requirement.	ESARR 4	Risk Assessment and Mitigation in ATM
Eurocontrol	Guidance	EAM 4/ GUI 1	Explanatory Material on ESARR 4 Requirements
FAA	Advisory Circular	25.1309-1A	System Design and Analysis
FAA	Advisory Circular	23.1309-1C	Equipment, Systems, and Installations in Part 23 Airplanes
FAA	Guidance		The FAA and Industry Guide to Product Certification (2nd ed)
FAA	Guidance		FAST - The Federal Aviation Administration Acquisition System Toolset
FAA	Handbook		FAA System Safety Handbook
FAA	Manual	Version 1.2	Federal Aviation Administration Safety Management System Manual
FAA	Order	1100.161 Chg 1	Air Traffic Oversight
FAA	Order	N JO 1800.2	NAS Change Proposal (NCP) Process Support of the Safety Management System
FAA	Order	1800.66	Configuration Management Policy
FAA	Order	3400.3H	Airway Facilities Maintenance Personnel Certification Program
FAA	Order	8000.9	AOV Credentialing and Control Tower Operator Certification Programs
FAA	Order	8110.4C Chg 1	Type Certification
FAA	Order	8130.2F	Airworthiness Certification of Aircraft and Related Products
FAA	Order	8000.368	Flight Standards Service Oversight
FAA	Order	8000.90	AOV Credentialing and Control Tower Operator Certification Programs
FAA	Order	80404.4	Safety Risk Management
FAA	Order	8100.5A	Aircraft Certification Service - Mission, Responsibilities, Relationships, Programs
FAA	Order	8130.2 Chg3	Airworthiness Certification of Aircraft and Related Products
FAA	Order	8110.42C	Parts Manufacturer Approval Procedures
FAA	Order	8120.2F	Production Approval and Certificate Management Procedures
FAA	Order	8150.1B	Technical Standard Order Program
FAA	Order	8260.19C	Flight Procedures & Airspace
FAA	Order	8260.3B	United States Standard for Terminal Instrument Procedures (TERPS)
FAA	Order	8900.1	Flight Standards Information Management

			System (FSIMS)
FAA	System Spec	SR1000	NAS System Specification
ICAO	Manual	Doc 9859, AN/460	Safety Management Manual (SMM)
ICAO	Guidance	Doc 9689, AN/953	Manual on Airspace Planning Methodology for the Determination of Separation Minima
Mineta Commision	Policy		National Civil Aviation Review Commission
RTCA, Inc	Process	RTCA/DO-254	Design Assurance Guidance for Airborne Electronic Hardware,
RTCA, Inc	Process	RTCA/DO-264	Guidelines for the Approval of the Provision and Use of Air Traffic Services Supported by Data Communications
RTCA, Inc	Process	RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certification
SAE	Process	ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

Appendix C

Interviews Conducted

Name	Title & Organization	Date (s) Interviewed
James Brady	Aerospace Engineer, FAA Small Airplane Directorate, Standards Office	4/17/2007
Mike Castle	ADS-B Separation Standards Analysis Group, Johns Hopkins University	4/25/2007
Bruce DeCleene	Aerospace Engineer, Avionics Systems, FAA Aircraft Certification Service	5/10/2007
Luke Cropsey	Manager, DoD Joint Integrated Product Team for UAS Airspace Access	7/20/2007
Lowell Foster	Flight Test Engineer, FAA Small Airplane Directorate	4/20/2007
Vince Galotti	Manager, Air Traffic Management, International Civil Aviation Organization	5/14/2007
Steve Thompson	Staff Member, MIT Lincoln Laboratory	5/11/2007 7/16/2007
Steve Van Trees	Manager, Avionics Systems, FAA Aircraft Certification Service	5/10/2007
Steve Vail	Senior Manager, Air Traffic Operations, Fedex Aviation	4/17/2007

Appendix D

Case Studies

The framework introduced in Chapters 6 and 7 is used to analyze case studies of implemented and pending system changes. The purpose of this chapter is to describe the relevant safety assessment and operational approval activities for each case and discuss identified implications trends and implications for future changes. The case studies and assessment methods is shown in Table D-1. Each of the three safety assessment approaches from the previous chapter was used in at least two cases. As the reader may also note, some cases used multiple safety assessment approaches.

Table D-1: Assessment Methods Used in Case Studies

No	System-Level Change	Implemented Year	Assessment Methods
1	Instrument Landing Systems (ILS)	1961	TLS
2	North Atlantic Organized Track System (NAT OTS)	1966-1981	TLS
3	Traffic Alert and Collision Avoidance System (TCAS)	1993	TLS (Risk Ratio)
4	Precision Runway Monitor (PRM)	1997	TLS
5	Automatic Dependent Surveillance, Broadcast (ADS-B) Alaska Capstone	1999	Risk Matrix
6	EUR Reduced Vertical Separation Minima (RVSM)	2002	Risk Matrix TLS
7	Automatic Dependent Surveillance, Broadcast (ADS-B) Segments I and II	(pending)	Risk Matrix TLS Performance-Based
8	Unmanned Aircraft Systems (UAS)	(pending)	Risk Matrix TLS Performance-Based

The discussion of each case will begin with an overview and description of the proposed change. Following this, the safety assessment approach used will be discussed along with key details regarding the approach framed using the safety assessment model and influence framework. Finally, key trends identified in the case and implications for future changes will be discussed.

D.1 Initial Instrument Landing Systems (ILS)

D.1.1 Overview and System Description

In the early 1960s, the British Civil Aviation Authority (CAA) implemented one of the first widely used quantitative targets as the basis for evaluation of a combination of airborne and procedural capability. Quantitative targets were used to evaluate the performance of Instrument Landing Systems (ILS) [105] [106] installations on aircraft. Instrument landing systems rely on a ground-based radio signal that defines the approach path to a runway in poor visibility. Avionics onboard the aircraft receive the ILS signal and provide guidance to the pilot, or are directly coupled to an autopilot system.

D.1.2 Safety Assessment Approach and Details

Development of ILS was one of the first cases of the use of a Target Level of Safety (TLS). A single risk level was derived as a safety target for the rate of accidents on approach. From this target, multiple additional targets were decomposed for subsets of system performance.

Derivation of the Target Level of Safety. The risk budget used to define the TLS is shown in Figure D-1 and has been adapted from [106]. At the time of implementation, the observed accident rate on approach was on the order of 0.6 accidents in every 10^6 landings. Judging the time exposed to ILS risk, a target for both performance and failures of the system was arrived at of 1×10^{-7} accidents / hr [105], which is the top-level event of the risk budget. The overall accident rate was allocated to performance and failure conditions equally, resulting in a performance target of 0.5×10^{-7} accidents / hr used to design the properties of the system. The performance target is further expanded in the figure. Within this target, risk was further decomposed to dimensions of performance (longitudinal and lateral), and then parameters of the system (longitudinal position, vertical velocity, etc). Each of these divisions served as targets for analysis of the decomposed modes of operation of the system.

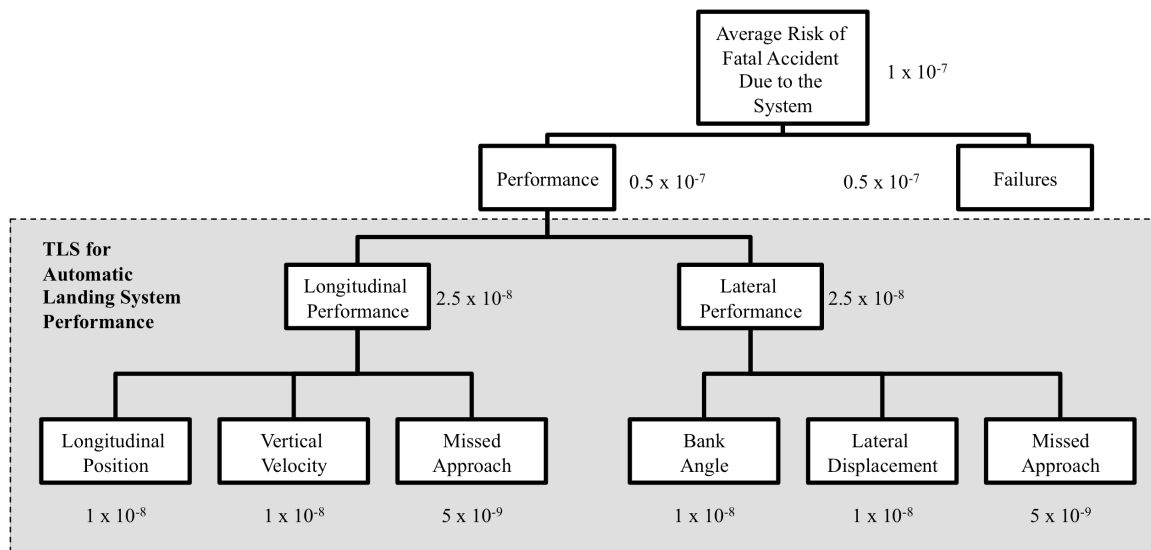


Figure D-1: Risk Budget for Automatic Landing Systems (modified from [105])

Associated Scope and Detailed Modeling and Assessment. Detailed simulations were used to simulate approaches and design parameters of the autoland system. Fault tree analysis was used to design failure modes to meet the target. The scope of assessment was focused heavily on technical performance of the system. Both technical and human failures were evaluated as part of the fault tree model [105]. Scope was further limited to risks of ground impact during approach. Other modes of flight and other risk events were not evaluated.

D.1.3 Discussion

The risk budget used in ILS was the basis for establishing risk matrices as acceptability criteria. As the basis for risk matrix criteria, it was pessimistically assumed that there were 100 safety-critical systems in an aircraft that could result in an accident ($n = 100$). The overall goal on accident rates was 10^{-7} accidents / hr, an improvement in the current level of experienced safety. By this reasoning, the likelihood of any individual failure leading to an accident was prescribed as 10^{-9} failures /hr.

From the catastrophic severity target of 10^{-9} , additional targets were established for lower severity risks, decreasing by an order of magnitude for each target. This approach was incorporated into early British Civil Airworthiness Requirements (BCAR) and became the basis for the Joint Airworthiness Requirements 25.1309 [106] and similar FAA requirements [58] for aircraft system installations.

D.2 North Atlantic Organized Track System (NAT OTS)

D.2.1 Overview and System Description

The ICAO North Atlantic region (NAT) is an oceanic control region with high traffic density between Europe and North America. To facilitate procedural separation of traffic, routes (known as “tracks”) are created at regular intervals based on forecasted winds. These tracks are known as the Organized Track System (OTS). Because of the lack of radar coverage over the ocean, traffic is surveilled through self-reported position. This makes collision risk highly dependent upon the navigation performance of individual aircraft.

Over several years, lateral, longitudinal, and vertical separation standards of the OTS have been reduced to accommodate increases in traffic and enable more efficient routing. Based on the use of collision risk assessment, NAT OTS spacing was changed three times from 1964 to 1981—twice in the lateral dimension and once in the longitudinal dimension. The analysis of NAT OTS separations will be limited to the evaluation of the two lateral separation changes, implemented in 1971 and 1981.

In the discussion, the TLS analysis approach is described first. After this, a background on each change to separation and key factors describing the change is provided. This serves as a basis for discussion of trends in the TLS method as applied to the NAT OTS.

D.2.2 Safety Assessment Approach and Details

North Atlantic Track spacing was evaluated using a Target Level of Safety (TLS) approach based on a risk budget used to decompose the target risk event as a loss of vertical separation. The TLS approach was used because safety behavior could be decomposed into an independent set of hazards contributing to a midair collision. Specifically, midair collision risk models decomposed a loss of planned separation by three dimensions of operation: lateral, longitudinal, and vertical. The independent decomposition allows evaluation of a loss of separation from the nominal case in a given dimension. For example, a loss of vertical separation occurs when aircraft were expected to be separated vertically and occupy the same position lateral and longitudinal to each other. An example condition is two aircraft separated by altitude, but following identical routes at the same speed and position.

A summary of NAT separation changes reviewed is shown in Table D-2 along with the overall risk goal and target levels of safety used. The initial evaluation of NAT spacing is noteworthy as the first reference to a TLS as the acceptability criterion and the first application of a quantitative midair collision risk model.

Table D-2: Summary of NAT Lateral Separation Cases Reviewed

Year	Separation [lateral (nm)/ long min)]	Risk Goal (accidents / hr)	Target Level of Safety
1964	120 / 15	(n/a)	(n/a)
1968	90 / 15	4.5×10^{-8} to 1.2×10^{-7} [107]	1.5 to 4×10^{-8} [107]
1971	120-60 (composite) / 15	4.5×10^{-8} to 1.2×10^{-7} [107]	1.5 to 4×10^{-8} [107]
1981	60 / 15	6×10^{-8} [107]	3×10^{-8} [93]

Risk Budget and Scope. The risk budget used to derive the NAT TLS decomposed a midair collision event to enroute midair collision, and then to an equal division of risk level by dimension of exposure (lateral, longitudinal, and vertical). This division is illustrated in Figure D-2. In addition, two primary factors were evaluated that influence risk in the lateral dimension: navigation performance (of aircraft) and gross navigation errors, caused by airborne or ATC-based operational errors.

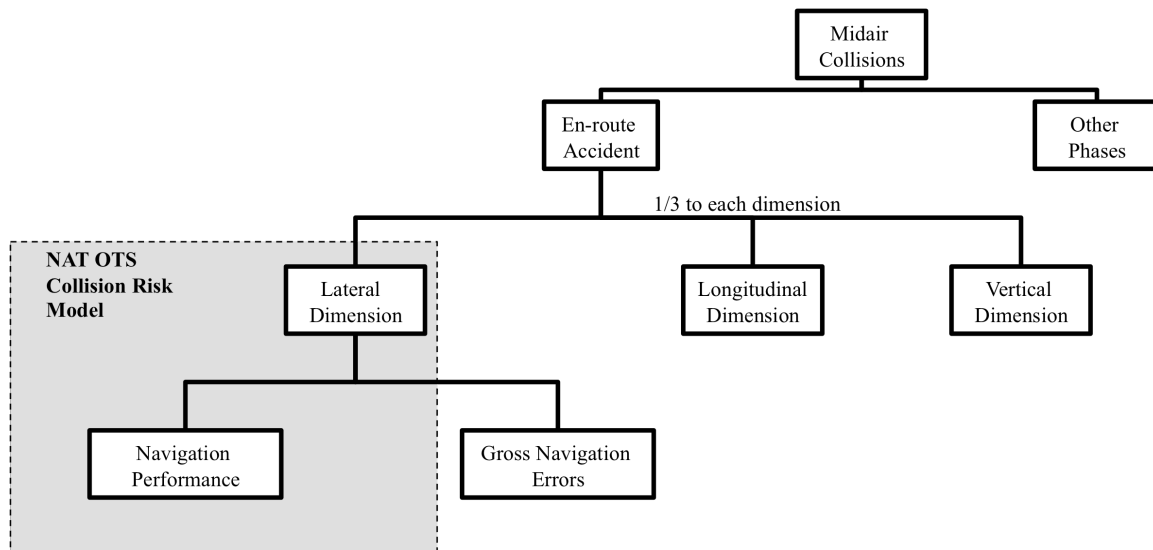


Figure D-2: Risk Budget Decomposition of NAT Collision Risk

The risk budget decomposition inherently limits scope to the risk event for which the target level of safety is defined. This eliminated consideration of other risks, such as loss of control or ground impact as well as system elements that contribute to the risk. The limit in scope was

consistent with the change being evaluated, namely to lateral navigation performance and airspace design in the lateral dimension.

Detailed Modeling Approach Used. To resolve deficiencies in the data and stakeholder disputes surrounding it, a quantitative midair collision risk model was created. The model was initially developed by Marks [108], and later refined and published by Reich [109]. The model is known generally as the Reich or Reich-Marks model [110]. Details of the collision risk model were refined over the course of evaluating several separation changes, but the basic structure of the model remained the same

The Reich-Marks model represents an aircraft by its gross dimensions of width, length, and height, and determines the probability of overlap of two aircraft based on the position uncertainty distribution. The model considers probability of errors in lateral, longitudinal, and vertical dimensions to be independently distributed. By this formulation, the probability of collision is the combination of probability of overlap in each dimension [90]. The model considers navigation error distributions, and neglects ATC-related operational errors [107].

Initial Models Used to Evaluate Collision Risk

In the early 1960s, NAT separation standards were 120 nm laterally and 20 min. longitudinally. Operational experts based these separations on judgments of navigation error distributions. The judgment that navigation errors followed a Gaussian distribution with mean zero. Safe lateral separation was assumed to be around two or three standard deviations from the mean, and the standard deviation was estimated largely based on expert judgment [107]. Observations proved that this was a poor estimate of actual collision risk [107]. It was noted by the planning group that collision risk was heavily dependent upon the tails of navigation error distributions, and a Gaussian model did not accurately account for the predominance of errors with significant deviation from the mean [111]. These deficiencies led to the development of the Reich-Marks Model.

Application of the Collision Risk Model to 1971 Separation Reduction

In the early 1960s, airlines made a request to ICAO to reduce lateral separation to 90 nm. To analyze this reduction, radars were installed by the FAA bordering the NAT region and on ships and data were collected from 1962-1963. The resulting analysis concluded that aircraft did not spend a substantial amount of time deviating beyond 45 nm (half of the separation), and it was expected that the reduction would be safe [90]. When ICAO moved to implement separation, the pilot organization refused to accept the safety argument, believing the data were not consistent with their observations. A resulting hearing in 1966 held by the FAA resulted in the removal of initial approval of separation, based on challenges to the observed data [90].

Additional data were taken on aircraft navigation distributions to represent sufficient accuracy to characterize distributions [107]. A target level of safety was used to evaluate collision risk in reduced separation based on the application of the collision risk model and navigation distributions. The initial risk goal was set 10 times below the observed midair collision rate for all aircraft (not just NAT traffic). This was to place a buffer for expected future growth in operations. Agreement was not achieved around a set number, but a resultant range of 4.5×10^{-8} accidents/hr to 1.2×10^{-7} accidents/hr [90] was reached. After decomposition, the resulting target level of safety was 1.5 to 4×10^{-7} accidents/hr [107].

Based upon the analysis of the model, the proposed 90 nm separation was deemed to be less safe than the required target. Participants recognized that this analysis only augmented judgment, and based on the assumptions made, the change may actually be safe in practice [90]. However, 90 nm separation was rejected due to the potential for operational errors in misunderstanding of cleared position. It was desirable to have tracks spaced in increments of 60 nm or 1 degree of latitude. This decision used judgment to evaluate a risk that was out of the scope of the mathematical analysis.

With this consideration, the analysts considered staggered separation [90]. This separation has aircraft pairs at the same altitude separated by 120 nm, but pairs 1,000 ft above separated 60 nm from those below. Staggered separation was implemented in 1971.

Establishment of Minimum Navigation Performance and Further Separation Reduction

After the introduction of composite separation, airlines requested a further reduction in lateral separation to 60 nm. In analyzing lateral performance data of aircraft in composite separation, several gross navigation errors were found well outside normal performance bounds that were not reflected by the assumed distributions [112]. This also resulted in a small proportion of traffic introducing a significant portion of collision risk.

In response to the pilot request, the NAT SPG re-evaluated the lateral target level of safety and further reduced it to 2×10^{-8} [107]. In addition, the original Reich-Marks model was refined to increase the sophistication by accounting for, among other factors: diverging aircraft at the exit of tracks and temporal variations in the distribution of errors due to inertial navigation.

In 1975, it was proposed by the planning group to implement the Minimum Navigation Performance System (MNPS) airspace, for which aircraft navigation systems were certified to specific performance boundaries. At the same time, the military planned to eliminate long-range navigation aids, necessitating a change in aircraft navigation system equipment [90]. Certification of navigation performance was expected to eliminate large variations in technical performance due to equipment errors. Without these changes, 60 nm separation was not deemed safe.

NAT MNPS was implemented by ICAO in 1978 and a monitoring program was instantiated to collect operational data [112]. As part of the monitoring program, it was found that aircraft complied with assumed performance, but that errors due to misunderstanding of ATC commands were creating deviations well outside of the assumed boundaries [107]. The errors were predominately due to misunderstanding of ATC command and therefore called “ATC loop errors [107].” These primarily resulted in mis-assignment to tracks. These causes were addressed through operational training, and not directly incorporated into the collision risk model. As operational error causes were addressed and MNPS equipment was implemented, 60 mi. separation was deemed acceptable and implemented in 1981 [112].

D.2.3 Discussion

The purpose of creation of the Reich-Marks midair collision risk model was to provide structure to the analysis of the safety implications of a change. This structure resulted in a common basis for a decision accepted by multiple stakeholders involved. As such, the stakeholders also realized that the initial quantitative analysis was a guide, discounting results due to assumptions and uncertainties. As time progressed, the Reich-Marks model's sophistication was increased, and more representative operational data were applied. This transformed approval decisions made on the model as more reflective of the operational environment, and gradually reduced the level of judgment applied to model results. Thus, the trend in use of the model was initially to advise judgment, and then became the key determinant of acceptability.

The initial assumptions on the independence of navigation errors by dimension persisted throughout the analysis. As will be seen in the RVSM case, the budgeted breakdown to independent dimensions continued to be used. Therefore, initial framings of a problem through quantitative models can persist for long periods of time and analysis of multiple systems.

With both increasing demands in safety performance and demands for reduced separation, derived requirements on navigation system precision increased. Initially, the baseline navigation system performance was used to determine required procedural separation. Later, the approach was inverted. Requirements were derived on equipment performance to meet procedural demands.

One of the most important insights from the NAT case study is that the scope of analysis expanded. In two cases, operational data forced the revision of assumptions as the basis for a prior approval. This indicated that aircraft navigation performance was no longer the dominant cause of midair collision risk. Errors were not normally distributed as initially assumed, prompting increased sophistication in data collection to support the 1971 reduction. Following that reduction, monitoring revealed gross navigation errors far outside of normal performance, and these errors were addressed.

In this case, the scope of causal factors increased, beyond baseline navigation performance, to include air traffic control interaction with aircraft. In addition, as dominant causes of risks were mitigated, other the magnitude of the influence of other causes became more significant, prompting the causes to be addressed.

D.3 Traffic Alert and Collision Avoidance System (TCAS)

D.3.1 Overview and System Description

The Traffic Alert and Collision Avoidance System (TCAS) is installed on aircraft to prevent midair collisions. The system is alternately referred to as the Airborne Collision Avoidance System (ACAS) by ICAO and Eurocontrol. TCAS determines the position of transponder-equipped aircraft through measurement of relative bearing and range computed from interrogation of other aircraft transponders. Altitude is encoded in the response for a class of transponders. Coupled with a set of collision avoidance logic, TCAS can also provide Traffic Alerts (TAs) to the position of other aircraft, and resolution advisories (RAs) to prevent midair collisions through commanded vertical maneuvers. Surrounding traffic, as well as TA and RA information is displayed to the pilot. TCAS I provides TAs only. TCAS II provides both TAs and RAs.

TCAS equipage was mandated by Congress following the collision between a DC-9 and general aviation aircraft near Cerritos, CA in 1986. It is the result of a concept originally envisioned and developed beginning in the 1950s [113]. TCAS II was mandated in the U.S. for turbine air carrier aircraft with greater than 30 seats in December 1993. Aircraft with 10 to 30 seats are required to be equipped with TCAS I [57], which only provides traffic alerts. Since 2005, TCAS II has been mandated worldwide on all aircraft with takeoff weight greater than 5700 kg or with 19 or more seats with exceptions granted for state aircraft.

D.3.2 Safety Assessment Approach and Details

Initial development of TCAS algorithms and evaluation of safety performance was conducted by the MITRE corporation with involvement of MIT Lincoln Laboratory, and documented in a system safety study [114]. Several follow-on activities were undertaken to further refine safety findings by MITRE and to update the TCAS logic [115]. Additionally, from initial certification and development, TCAS software has been refined to address issues that have been identified

through operational use [115]. The analysis of this case will focus on details of the initial system design decisions and safety assessment conducted by MITRE [114] and will then include some of the emergent issues and analysis associated with major updates to the system.

Analysis of TCAS followed the TLS approach. The criterion used was not an expression of level of risk, but a relative measure of risk in the form of a risk ratio. The ratio was defined as the risk level of a near midair collision (NMAC) with TCAS compared to the risk level without TCAS. An NMAC was defined as aircraft that approach as close as 100 ft vertically and 500 ft. horizontally [114]. No formal requirement was placed on the risk ratio. It was clearly desirable that the risk ratio be less than 1, indicating that implementing TCAS would reduce the risk level of midair collisions.

An NMAC was chosen as the target event instead of a midair collision because the occurrence of a midair collision depends on several factors related to relative geometry of collision and size of aircraft. These are difficult to quantify analytically. Instead, a near-midair collision of very small separation is reasonably close to the event of concern and does not need to account for detailed aircraft geometry.

D.3.3 Initial System Safety Study

The initial assessment of TCAS safety performance was conducted by a team led by MITRE [114]. The core of the safety study was an extensive fault tree with detailed conditions evaluated leading to a potential NMAC. The initial construction of the fault tree represented a scoping decision regarding the key elements and conditions leading to the NMAC risk. It was also used to evaluate complex causal relationships in the detailed assessment and mitigation process. The fault tree was quantitatively analyzed to determine the expected risk ratio under nominal conditions, and parameters were also varied to assess sensitivities to assumptions and the effect of potential failure modes.

Several other activities were used to derive parameters for evaluation through the fault tree. Modeling fault tree parameters was based on judgments by the MITRE team and operational experts and data from early operational trials with developmental versions of TCAS. Data were obtained from airline-recorded data on trials with Piedmont Airlines, flight trials around Atlantic City with an FAA aircraft, radar observations from NASA Wallops, and incident reports on

NMACs collected by the FAA. Combined, this data represented a small set of experience compared to what would be accumulated with future significant TCAS equipage. The data set was limited by the ability to process large amounts of radar data, and the sensitivity of attaining airline operational data from commercial carriers [115].

Scope of Analysis Due to TLS Approach

Events other than an NMAC were not considered analytically. The exclusion of ground impact in the analysis was subject of considerable debate during the course of analysis [115]. The initial assessment was performed under the assumption that a resolution advisory could only influence the risk of a ground impact under cases of rapidly changing terrain, and it was expected that these would be rarely encountered in operational service. Thus, the overall influence of the design parameters on ground impact risk was judged to be weak, and the result level of risk affected was scoped out as negligible. Terrain avoidance alerts and maneuvers were also given higher priority than TCAS.

Using a risk ratio approach also scopes the analysis to events that occur after a potential conflict already exists. Events and associated system elements that result in a loss of procedural separation or failures are therefore eliminated from scope. By not quantifying to an absolute level of midair collision risk, the rates of occurrence of initiating events were not modeled.

Similarity was also inherently applied using the risk ratio approach. Evaluating both the baseline system and the system with TCAS measures a relative effectiveness, rather than an absolute level of risk. This assumes that the systems after implementation and before behave in similar ways, scoping out any potential behavioral differences and embedding them into the detailed risk model.

Because TCAS resolution advisories are issued in the vertical dimension, horizontal encounter characteristics between aircraft were evaluated only as they related to the likelihood of proximity for collision in the vertical dimension, and horizontal miss distances were assumed to be uncorrelated to vertical miss distances. This scoped out the evaluation of any horizontal dynamics influenced by TCAS.

Scope of System Elements Considered in the Design

The initial TCAS safety study identified several system elements to include. These included the change elements of: TCAS equipment and collision avoidance logic. There were also several elements considered with which TCAS interacts, with the associated behavior included in the fault tree. The elements considered in the initial assessment are discussed below. It is important to note that many of the assumed properties of the elements were later re-evaluated in subsequent assessments of TCAS effectiveness. These issues will be discussed separately in the following section.

The TCAS avoidance logic is a critical change factor influencing its performance. Several parameters were used to vary designed logic, and compute resolutions that would maximize separation and be robust to disturbances.

TCAS was designed to be effective in encounters with other TCAS-equipped aircraft, as well as aircraft equipped with the Mode A and C transponders of the time. Mode A transponders do not encode altitude, therefore information based on signals received provided only relative bearing to aircraft, and only traffic alerts are provided. Mode C transponders encode altitude, and signals from Mode C equipped traffic are used to provide resolution advisories. Encounters with each element were considered separately as strong influences in their contribution to the effectiveness of TCAS. The transponder equipage fraction of other aircraft was an important factor and was also considered as a property of each system element.

TCAS relies on the pilot to interpret and execute responses to traffic alerts and resolution advisories. This includes pilot ability to visually detect aircraft when conditions permit. Thus, the pilot was a system element with a strong influence on the effectiveness of TCAS. In evaluating nominal performance, the safety study assumed complete compliance in pilot responses to RAs in calculating a risk ratio. However, sensitivity analyses were performed to evaluate the effect of assumed rates of pilot non-compliance with RAs [115]. The visual acquisition function of the pilot was also modeled, in having an effect in mitigating the risk of encounters with altitude unknown targets and in augmenting RA behavior. Pilot behavior was

also qualified by a degree of similarity to current operations. TCAS was expected to function similar to controller traffic and resolution advisories.

Several potential failure conditions in interaction with other aircraft were included. Examples include bit errors in encoded altitude and inaccurate altitude reporting. In addition, the flight behavior of other aircraft was considered, including sudden “deceptive maneuvers” which could lead to an induced collision or a reduction in effectiveness of TCAS interactions.

Failures within the TCAS surveillance system, such as loss of surveillance tracks were also included in the analysis, as well as TCAS system reliability based on an assumed mean time between failures. Failures were scoped to those that were judged to related directly to the rate of NMACs, and did not include any failures that could degrade situation awareness.

As TCAS is considered to operate independently from ATC, ATC functions and interaction with ATC commands were scoped out of analysis. This was under the rationale that TCAS alerts would have priority over ATC commands, and pilots would inform ATC of resolution actions after being clear of conflict. Although scoped out of analysis, a branch was maintained in the fault tree to later account for controller instructions and response to controller conflict advisories. However, this branch was not evaluated, and does not include the potential for conflicting instructions between TCAS and controllers. The exclusion of ATC had a noteworthy effect on the validity of analysis, as interactions were later found to be significant, as will be discussed in the following section.

Detailed Assessment and Mitigation

Estimates of key parameters were used to characterize the performance of the system elements described above. Examples include estimates on environmental conditions (i.e. IMC/VMC), equipage fraction of aircraft with transponders, distributions of intruder aircraft by altitude, and errors in transponder-reported altitude. In addition, observed responses to traffic and resolution advisories by the trial flight crews were used to validate assumptions on the pilot-commanded climb rates, altitude deviations, and subsequent level-off maneuvers [115].

Where uncertainties existed in model parameters, sensitivity analysis was conducted for each parameter independently to ensure that it did not significantly alter the risk ratio. Parameters

were also weighted to represent an average flight condition. With this weighted average, the risk ratio expected in service was calculated as 42%, meaning the implementation of TCAS would result in a risk level of midair collisions that was 42% of the rate without implementing TCAS.

The model also provided insight into training implications for flight crews, which were deemed necessary. These included compliance with RAs and maintaining vigilance in visual acquisition to avoid complacency. These represented safety-derived requirements necessary to mitigate a reduction in TCAS effectiveness.

Operational Approval

The development of standards for TCAS was performed within an ICAO working group, the SSR Improvements and Collision Avoidance Systems Panel (SICASP) [115]. The group was used to vet assumptions and system studies analyzing the effectiveness of TCAS, and ultimately made recommendations to ICAO regarding the incorporation of TCAS into ICAO Standards and Recommended Practices (SARPs). The SICASP held multiple sessions throughout the development and refinement of TCAS to address issues in logic and plan early implementation and final standards. A detailed summary of these decisions has been prepared by Carpenter [115].

The SICASP analysis was conducted in parallel, and was related to, FAA decision-making to mandate the implementation of TCAS [116]. However, details on FAA and other countries' operational approval decisions were not readily available.

D.3.4 Further TCAS System Refinement and Studies

After the initial system safety conducted by MITRE, the data gathered in operational trials and in operational experience was found to conflict with some initial assumptions. The original MITRE study was reassessed and several design changes to the TCAS algorithm resulted. The identification of issues after the initial study does not detract from the validity of the initial study in the context of limitations in available data. However, understanding the decisions made regarding these issues provides insight into limitations in safety analysis, including underlying data used in modeling and initial scoping decisions. A subset of issues identified are discussed below, organized by the major revisions to TCAS software that resulted or are expected to be implemented after addressing the challenges.

Refinement of Initial TCAS Logic to Version 6.04. Simulations of TCAS logic based on radar observation of operational trials of TCAS in 1987-1989 challenged some assumptions made as part of the initial MITRE studies [115]. In particular, assumptions made regarding the independence of horizontal and vertical properties of encounters were found to be too simplistic and not representative of the behavior of aircraft under ATC control.

Re-evaluation by panel experts judged the existing logic to be safe, even under modified conditions. During the course of the re-evaluation, several changes were made to CAS logic to improve the performance in encounters between two TCAS-equipped aircraft, and reduce the number of nuisance advisories in ATC [117]. Additional correction of a specific encounter scenario, known as the “Seattle encounter” also resulted in modifications to CAS logic to reduce risk in encounters identified in interaction with Air Traffic Control commands [117]. The resulting version, 6.04A was mandated by the FAA in 1994 [118].

Development of TCAS II, Version 7.0. Additional operational data and increases in computational power allowed a more sophisticated analysis of potential encounter scenarios to serve as a basis for a major improvement in TCAS performance to Version 7.0.

Throughout the operation of TCAS, radar data had been collected that was used to statistically characterize aircraft dynamics before a close encounter. These served as a basis for development of an FAA technical center simulation analyzed by MIT Lincoln Laboratory (MIT LL). TCAS performance was characterized under conditions more representative than the parametric MITRE study. The model used Monte Carlo simulation techniques based on conflict parameters to evaluate TCAS logic versions 6.04 [117] and 7.0 [118].

Several changes were implemented in Version 7.0. Sense reversals, or a change in direction of resolution advisories were modified to increase separation under conditions when other aircraft did not comply with TCAS alerts. Horizontal filtering was added to reduce false alerts when aircraft had sufficient horizontal separation. Also, logic regarding multiple aircraft encounters was redesigned.

D.3.5 Emergent Issues in Current TCAS Implementation, Version 7

Additional issues have emerged in concern with the currently implemented Version 7.0, prompting efforts that have resulted in the modification of TCAS to Version 7.1. Two emergent issues are discussed below.

Sense Reversals for Non-Compliant Intruders. In some conditions, conflicting commands between air traffic control and TCAS resolution compliance can result in the situation illustrated in Figure D-3. Illustrated in this scenario, TCAS issues a resolution advisory to the first aircraft to descend. A second aircraft receives ATC instruction to descend at approximately the same time. Shortly thereafter, a climb RA would be issued by TCAS to resolve the potential collision, with which the pilot does not comply. In Version 7.0, no reversal is issued to the first aircraft, potentially creating an induced collision. In version 7.1, the modified collision logic can detect the non-compliance of the second aircraft and issue a sense reversal, which is more likely to resolve the collision. This situation was identified as a contributor to a midair collision near Überlingen, Germany [119]. The resulting change proposal, CP112E has been analyzed and is in the process of receiving operational approval [120].

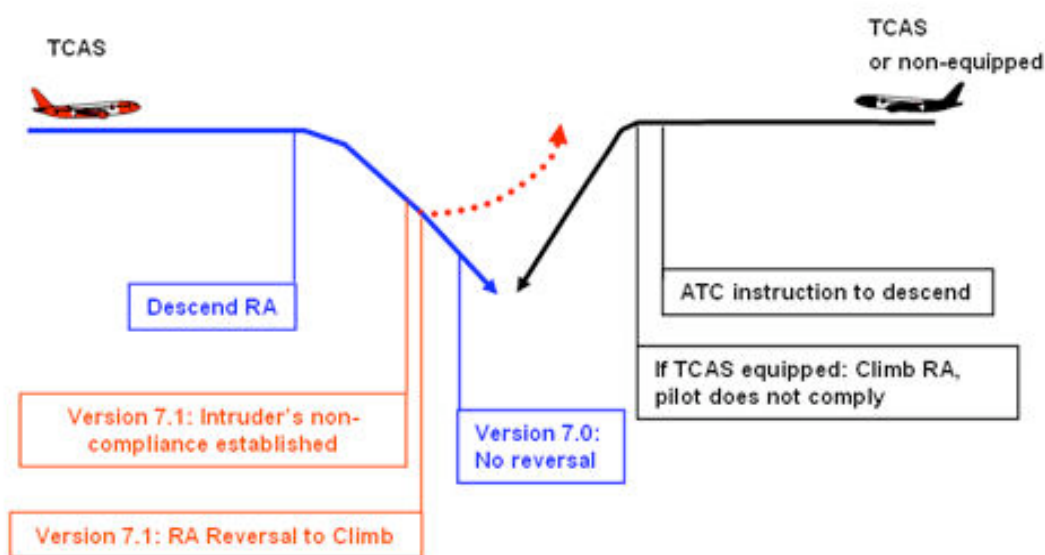


Figure D-3: Illustration of TCAS Rate Reversal Logic Change [121]

The lack of a downlink of TCAS behavior to Air Traffic Control is one contributor of the increased risk level of an induced collision. The presence of this risk level has prompted an analysis of the feasibility of downlinked TCAS resolution information to ATC [122].

Aural Alerting Phraseology. Another issue that has emerged is pilot reaction to the resolution command to adjust vertical speed, which is typically used to cue the pilot to reverse a rate of ascent or descent. However, the aural alert is confusing, and proposals are in place to replace it with a level-off command. [121].

D.3.6 Discussion

Use of Data and Assumptions. Parameters estimated in the initial system safety study were based on the engineering judgment of the assessors. Limited operational experience served to validate assumptions, but a significant lack of data and computational capability did not allow them to be incorporated accurately into the detailed models of the system. Instead, sensitivity analysis was conducted to examine the effect of key assumptions, and they were not found to significantly reduce the overall safety of the system.

Increased representativeness of operational data and sophistication of models has enabled logic changes and improved performance through software revisions. Although this operational data challenged assumptions made as the initial basis for TCAS approval, the architecture of the system has remained relatively constant over time, indicating that the initial design of the system was robust.

Role of Similarity. TCAS represented a fundamentally new operational capability. In TCAS, collision avoidance functionality was incorporated in an automation system onboard the aircraft under different conditions than previously used by pilots or air traffic controllers. It shifted a task of awareness of traffic from the ground and provided the capability to pilots. It also implemented resolution advisories in a shorter time to collision than available via air traffic control surveillance.

Although the capability was fundamentally new, in some aspects, the functionality was similar to current system operations. Resolution advisories were designed to mimic those given by

controllers under similar situations, but the shift in allocation was significant enough to require complete evaluation of the system.

Elimination of Air Traffic Control from Scope. One deficiency in the early architecture was the lack of broadcast information on TCAS resolutions to air traffic control. This represents a failure in the scope of initial analysis. While the analysis framework allowed ATC behavior to be incorporated as external to TCAS functionality, it did not provide a sufficient basis to merit an architectural design decision to provide TCAS information to ATC.

The counter-argument is that the architecture of TCAS as independent from ATC allowed changes to be incorporated without requiring substantial changes to other aircraft equipment, ATC, or ground infrastructure. This has allowed improvements to the system to be incorporated without requiring the creation of a new system.

Flexibility in Reconfiguration of System. Strong continued monitoring and development after operational implementation enabled the ability to further improve the effectiveness of TCAS. Changes to avoidance logic were and continue to be motivated by observed incidents [120]. This represents a valuable use of operational data to address precursors to accidents. Unfortunately, the Überlingen accident prevents an example where an accident highlighted and accelerated demands for change. The implementation of collision avoidance logic in software allowed flexibility in adapting to identified issues.

Embedded Judgment on Induced Collisions. It was recognized during initial development that the use of TCAS could induce some midair collisions. In the assessment of the system the tradeoff between induced and prevented collisions was incorporated into the model of the assessment, and not imposed externally through acceptability criteria. Early attempts to create separate risk ratios were proposed but failed [115].

TCAS As a Mitigation for Future Operations. TCAS performance can be often used to support the safety assessment of other changes to the system, providing mitigation against the risk of a loss of separation. Consider the three lines of defense commonly asserted as preventing a midair collision illustrated on the left-hand side of Figure D-4. A level of risk is present due to the density of traffic. Procedural separation further reduces risk by separating aircraft along

common routes. Additionally, air traffic control is responsible for separation of aircraft when observable and under their control. TCAS, where equipped, provides a second layer of collision avoidance protection. The final defense against a midair collision is pilot ability to see & avoid. A midair collision results in a failure of all defenses, either through lack of identification, or failure to resolve. The equivalent event tree, of the sequence is shown on the right side of Figure D-4:.

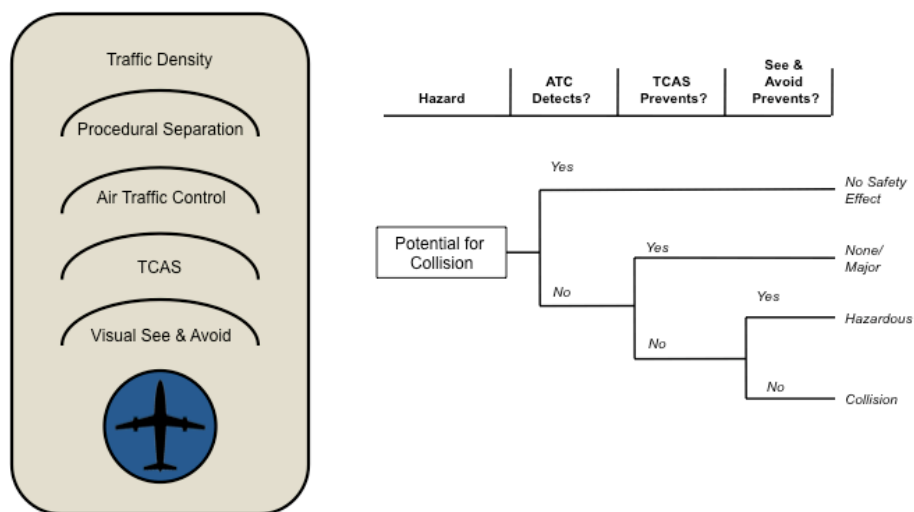


Figure D-4: Collision Avoidance Prevention Mitigations and Event Tree

An example of the effectiveness of TCAS is shown in Figure D-5 from Andrews, et al. [123]. The authors evaluated an advanced ground-based separation and alerting system, where faults introduced could result in a failure of conflict-free trajectories. TCAS was an element in the system model that reduced the expected rate of midair collisions under conflict scenarios. This effect is shown in the orange region, and is generally an order of magnitude reduction in the rate of collisions.

Without TCAS, increased performance would be required in other system elements to reach the same level of midair collisions. This unavailability of TCAS could be present due to a lack of equipage of other aircraft.

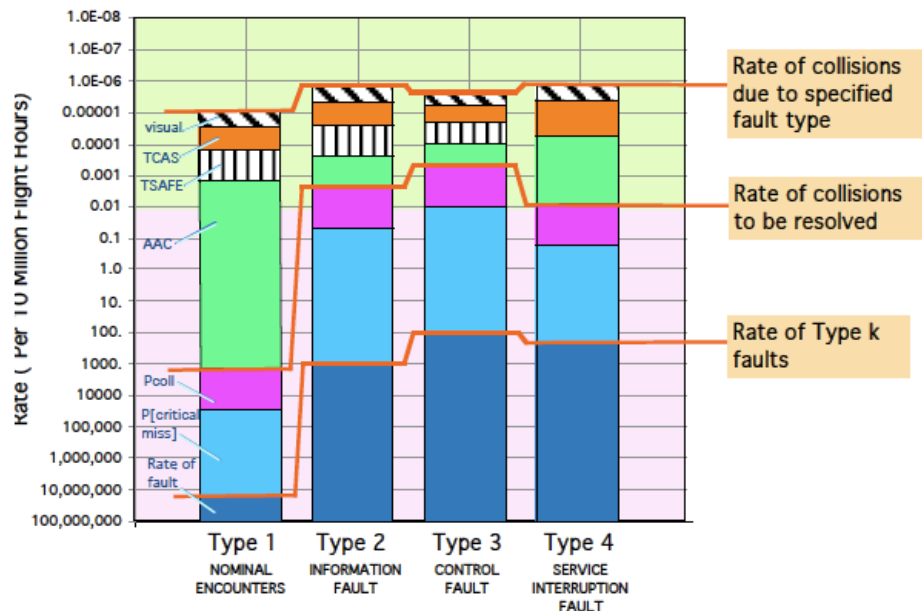


Figure D-5: Andrews, et al. Analysis Results of Advanced Separation Concept [123]

D.4 Precision Runway Monitor (PRM)

D.4.1 Overview and System Description

The Precision Runway Monitor (PRM) was designed to allow reduced lateral separation on approach to closely-spaced parallel runways. PRM increases capacity at some airports where runways are spaced too closely to permit safe separation using conventional terminal radar, between 3400 and 4300 ft (3000 ft with an offset ILS). The PRM system consists of high update rate radar and air traffic control display monitored by a dedicated controller. The controller uses the PRM display in Instrument Meteorological Conditions (IMC) to monitor aircraft deviations from their assigned approach paths. If a deviation is detected, the controller issues a breakout command to one or both aircraft on approach to avert a potential collision. The first PRM system was installed in Minneapolis and commissioned in 1997.

D.4.2 Safety Assessment Approach and Details

The TLS approach was used to evaluate and specify key system elements of the PRM system: the update rate and azimuthal resolution of the radar; distance between parallel runways; and dimensions of the no transgression zone (NTZ) [124]. The functionality of the system was judged to be sufficiently independent from other conditions that it was possible to scope the analysis to a single hazard: the potential for midair collision due to unresolved blunders.

The safety analysis supporting PRM design parameters was conducted by MITRE and published by the FAA in support of the acquisition of the system [124]. This case is based on the FAA report, and other references to PRM in literature [96, 107, 125].

Target Level of Safety and Risk Budget. PRM was designed to an equivalent level of risk to current operations, assuming the current level of accident approach risk was acceptable. To determine this target, NTSB accident data were reviewed for a six-year period. Divided by the assumed operating hours in IMC, this yielded the acceptable final approach accident rate of 1 accident per 2.5 million approaches [in IMC] or 4×10^{-7} accidents per IMC approach [124]. The risk budget breakdown for PRM is shown in Figure D-6.

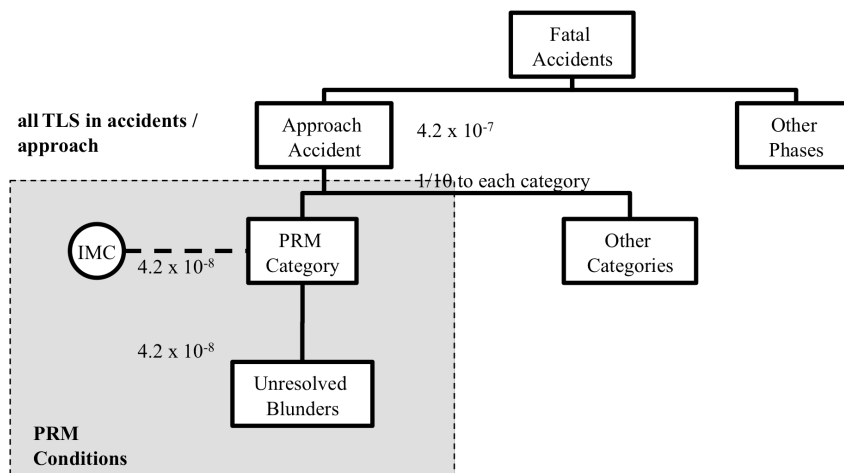


Figure D-6: PRM Risk Budget

From the overall final approach IMC accident rate, nine categories of final approach accidents were decomposed of which *failure of the PRM system* was expected to add a tenth cause. Only three causes are listed in the documented analysis (engine failure, collision with an obstacle, and aircraft deviation from the approved flight path) [124]. With this factor, the design goal for the PRM system is 1 accident per 25 million IMC approaches or 4×10^{-8} accidents per IMC approach. The nine causes of approach accidents were not directly observed. Only two accidents occurred during the period used to review safety [124]. Based on this, the $1/10^{\text{th}}$ factor represents a judgment of the fraction of risk that the PRM should assume as an equivalent contribution to other systems.

Detailed Modeling and Assessment. Documentation of the design process that resulted in the initial configuration of the PRM system was not available. Safety available studies document safety decision-making based on early operational trials of deployed PRM systems, as well as simulation and quantitative analysis. The quantitative assessment is the only aspect of analysis that related system performance to the risk target. However, the quantitative assessment was performed along with analysis of other aspects of the system. Therefore it is important to discuss both below.

Several system elements interact in PRM. Air traffic controllers utilize dedicated displays to monitor aircraft approaches and issue breakout commands. Pilots perform approaches, using autopilot and ILS equipment. In addition, TCAS provides awareness of other traffic, and can potentially issue traffic alerts or resolution advisories. Properties of the PRM procedures were also evaluated, including update rate and separation between runways.

One aspect of the safety study was to investigate the magnitude of flight technical error on ILS approaches for different aircraft types. This informed the boundary that aircraft were expected to deviate on an ILS approach, and set a minimum allowable separation distance between runways based on current ILS performance.

Simulations also informed judgments about pilot and controller response to blunders. Pilots were found to respond less aggressively than desired when issued breakout instructions, so requirements were placed to train pilots on breakout procedures. Controller behavior focused on assessing the influence proposed properties of the PRM system on performance in blunder identification and response time [125]. These studies also quantified parameters used in a Monte Carlo simulation of blunders.

In the trial and simulation results, the perceptions of controllers of the utility of the system were also probed through structured surveys. Both pilots and controllers were generally accepting of the midair collision protection afforded by the system [124, 125] and DOT. This approach elicited an implicit acceptability judgment by users, which supported operational approval.

TCAS was installed for test flights at two locations, and the interaction of TCAS and the PRM system was observed. It was found that TCAS RAs occurred frequently while aircraft were

maneuvering and acquiring the threshold. It was also found that TCAS augmented PRM breakout instructions in the case of a blundering aircraft, and it was judged that the operation of both systems in parallel did not significantly influence safety. Modifications were recommended to operate TCAS separately on parallel approaches, but they were not implemented [124].

The likelihood of midair collisions given a blunder was evaluated using a Monte Carlo simulation. This estimated that there was one midair collision, out of every 250 worst-case blunders. The risk analysis performed did not follow the conventional approach of modeling parameters and comparing results to a target level of safety. Instead, the target level of safety was set for performance of the system, and the acceptable rate of blunders was calculated. It was assumed that there was a 1% probability of a worst-case blunder, given that a blunder occurred. This resulted in an acceptable frequency of 1 blunder every 1,000 approaches. This was validated through anecdotal evidence on the rate of blunders at other facilities.

D.4.3 Discussion

While the scope of hazard to midair collision on final approach appears to have been made appropriately, it is not clear that worst-case condition of a blunder appropriately represents the worst-case system state for analysis. The blunder condition assessed was an aircraft changed heading 30 degrees into the path of the other aircraft executing an approach. As an initiating event, it was dismissed as an extremely rare event. Because of the low frequency, the PRM system was only required to add marginal mitigations designed based on a single case. It is not clear that more likely, but less severe events should not have been considered that would lead to midair collision risks [126]. Other failure modes using the system, such as misidentification by a controller, equipment failures, or even other blunder modes were not explored.

Instead of a direct reliance on the quantified risk of midair collision due to blunders, the simulations and flight trials performed likely created sufficient confidence in system capabilities to achieve operational approval.

D.5 Reduced Vertical Separation Minima (RVSM) in Europe (EUR)

The influence matrix was applied to the FHA of RVSM in Chapter 6. A system description and analysis of the risk matrix approach was included as part of the chapter. In this appendix, other key issues in the safety assessment of RVSM are discussed. The system description is repeated for convenience.

D.5.1 System Description

Under conventional separation minima, aircraft are separated vertically by 1,000 ft flight levels (FL) below FL 290 (29,000 ft) and by 2000 ft. above FL 290. This variation in vertical separation with altitude was due to the dependence of height-keeping on barometric altimeters. At higher altitudes, the same pressure accuracy of the altimeter translated to a larger altimetry system error due to the more shallow gradient of pressure with altitude.

Beginning in 1990, ICAO published draft guidance material [91], on the feasibility of reducing vertical separation in several regions. The operational reduction in vertical separation required increased altimetry precision, which was assured through certification to Minimum Aviation System Performance Standards (MASPS) on new and retrofitted altimetry systems.

From 1997 to 1998, RVSM was implemented in the ICAO North Atlantic Region [93]. Following this implementation, Eurocontrol performed a safety assessment supporting implementation in the European region (EUR). This safety assessment was conducted for the specific EUR operational environment, but built on standards on aircraft performance that were established earlier by ICAO. The change was approved and implemented in EUR airspace in 2002. RVSM has also been implemented in most other world regions, including the United States, but those implementations are not the focus of this analysis.

To support operational approval in the European Region (EUR), two safety assessments were performed, both before [94] and after [95] implementation. Each safety case considered transition areas to RVSM, and “core” RVSM airspace. The focus of this case study is on the assessment of mature airspace performed in the Pre-Implementation Safety Case (PISC) [94]. As part of the safety case, a Functional Hazard Assessment (FHA) was also conducted [92].

The discussion of this case will begin with a description of the safety assessment approaches used. Analysis of the case is then organized along the general processes of safety assessment: hazard identification and scoping, detailed analysis and modeling/ mitigation, and operational approval.

D.5.2 Collision Risk Modeling to TLS

Collision risk modeling was used to evaluate required altimetry system performance to the associated target level of safety. Risk was modeled using the ICAO close approach proximity model [127]. This model is an extension of the Reich-Marks model described in the NAT OTS case. The model relies on estimating a horizontal overlap rate based on traffic characteristics, and associated probability of vertical overlap due to height-keeping performance. ICAO established a Minimum Aviation System Performance Standard (MASPS) [128] for altimetry systems. The MASPS specified altimetry system performance in terms of three parameters: mean (80 ft), 3 standard deviations (245 ft), and integrity (probability of failure of 1×10^{-5}).

In early operational monitoring, the height-keeping performance of aircraft already equipped to the MASPS was monitored. The data were to statistically characterize altimetry performance of aircraft operating in the airspace. When correlated with ATC clearance data, the HMU results gave distributions both for altimetry system performance error, and “flight technical error” which was indicated vertical position errors due to deviations from clearance. Data also provided an estimated rate of horizontal overlaps [95].

The horizontal overlap and vertical error data were combined in a mathematical model to evaluate determine the expected collision risk due to vertical overlap. It was found that with current aircraft performance, expected level of risk was 0.5×10^{-9} . Data from operational errors were also included, finding an overall expected level of safety of 0.5×10^{-9} . Each value exceeded the corresponding TLS of 2.5×10^{-9} [95].

Elimination of TCAS from Scope

As discussed above, TCAS behavior was not directly assessed as part of the FHA performed. Instead, it was assumed that TCAS was qualified by similarity to lower altitude levels with conventional separation. Two hazards associated with interaction with TCAS were deemed unacceptable, and required additional monitoring activities.

The hazard “nuisance TAs and RAs” was not considered to meet the required safety objectives. Excessive climb and descent rates were judged to potentially initiate TAs or RAs. There were no RVSM-specific mitigation means determined by the assessors that could address the risk. Instead, a follow-on study was conducted by Eurocontrol and found the level of alerts to be acceptable [97].

The second hazard assessed as safety-critical (i.e. high risk) was “pilot is deviating from clearance.” This situation is commonly referred to as an altitude burst, which indicates that a pilot either deviates from the assigned altitude, or continues to climb or descend through an assigned altitude.

The level of risk associated with the hazard is dependent upon TCAS interactions, as well as potential operational errors by pilots or controllers. No mitigation measures were identified that could address the risk of deviation, although it is clear that RVSM system elements relate to it. Instead, it was argued that the risk exists and is tolerated in the current system, and the only effect of RVSM would be increased absolute frequency.

Although no mitigations were prescribed in the safety case, training programs were initiated by Eurocontrol to mitigate the risk associated with deviations. The follow-on Post-Implementation Safety Case [95], reassessed the risk and found it to be tolerable.

D.5.3 Discussion

The two methods used to determine safety-derived requirements in RVSM illustrate divisions in the applicability of the methods. The assessment to a risk matrix was performed using qualitative estimates of likelihood. It was also used as a means to derive requirements, which were best practices in addressing identified hazards: training, equipment design, and airspace design.

Where it was necessary to assess technical performance, a sophisticated midair collision risk model was required. This model relied on an accurate representation of operational data and related it directly to the level of midair collision risk. It was also used to assess the implications of observed operational errors.

TCAS was identified as a significant interacting element. TCAS had a strong influence on the identified safety critical hazards. These hazards were not mitigated through RVSM elements. Instead, their occurrence was monitored through follow-on activities. The monitoring program found behavior to be acceptable [97].

D.6 Overview of Automatic Dependent Surveillance, Broadcast (ADS-B) Cases

ADS-B is an integrated set of airborne and ground components that are used to transmit GPS-derived position and other information to the ground and other aircraft. This capability is known as ADS-B out. The presence of a datalink also enables the receipt of information from other aircraft and the ground, known as ADS-B-in. ADS-B has two corresponding services broadcast from the ground. Traffic Information Services, Broadcast or TIS-B contains information from surveilled traffic through ADS-B or rebroadcast from ground radars. Flight Information Service, Broadcast or FIS-B contains airspace information, and meteorological information, including graphical weather.

ADS-B uses two types of transponders to relay information. A transponder similar to a Mode S transponder with extended information is the 1090ES (extended squitter). 1090ES is expected to be adopted by large commercial aircraft. The Universal Access Transceiver (UAT) operates on

978 MHz and has higher bandwidth for receipt of graphical information, such as weather, and is expected to be attractive for equipage by General Aviation aircraft [129].

ADS-B was initially conceived as a replacement to radar-based surveillance, to enable the retirement of existing secondary surveillance radars. Since its initial development, the use of ADS-B has expanded to support multiple applications.

The analysis of ADS-B is divided into two cases. The first case focuses on the initial deployment of ADS-B as part of the Capstone program in Alaska, beginning in 1999. The Capstone program was an early demonstration of ADS-B functionality using UAT. The FAA subsidized installation on several aircraft of an ADS-B system that broadcast GPS-derived position to air traffic control, and provided a display to pilots of surrounding air traffic and terrain. The focus of this discussion is the hazard analysis supporting the implementation of radar-like services using ADS-B as a surveillance source [130]. A hazard analysis was also performed for other applications of ADS-B, but is not the subject of the Capstone case analysis [131].

The second case focuses performance requirements for system-wide deployment of ADS-B in the United States. As part of this deployment, there are plans to support multiple future applications relying on ADS-B. These plans are based on development of requirements for ADS-B performance for multiple applications that is currently in process in the US and internationally [132]. The FAA has published a notice of proposed rulemaking mandating equipage and performance requirements for ADS-B-out. Requirements for additional ADS-B applications have also derived through several safety studies. These assessments of required performance have been conducted by RTCA [133, 134] and by the ADS-B separation standards working group, as documented in open literature [135]. The case study will focus on a comparison between requirements for different applications.

D.7 Automatic Dependent Surveillance Broadcast (ADS-B) Alaska Capstone Program

D.7.1 Safety Assessment Approach and Details

A scenario-based preliminary hazard analysis was performed to evaluate expected safety performance to a risk matrix. The scenario-based assessment defines hazards as a set of operational conditions, grouped together into a scenario. Initial risk was categorized based on existing controls, and mitigations were evaluated qualitatively to reduce high risks to acceptable levels [130]. This process is discussed in the first section.

Additionally, during the course of the Capstone operational evaluation, concerns were raised regarding the dual use of ADS-B and radar targets for separation. This resulted in a disapproval of ADS-B information and required a reassessment of the safety assessment before returning the capability. This is discussed in the following section.

ADS-B-Out Hazard Analysis

The risk matrix used in the evaluation is shown below in Figure D-7. The structure of the risk matrix is noteworthy in two respects. First, with the exception of the catastrophic category, the severity categories and criteria differ from those typically used by the FAA. This is evident in contrasting Figure D-7 with the ATO SMS risk matrix shown in Figure 5-1. Second, the assessors recognize that the nature of Alaska operations allow risks that are typically ranked as high risk (i.e. in the region of catastrophic and extremely remote) to be accepted. This acceptance acknowledges the need to further evaluate the risks in operational practice, and it also acknowledges that scenarios with risk in the region have been improved by the introduction of Capstone equipment, and would not have initially been in the acceptable region.

SEVERITY LEVEL	LIKELIHOOD OF OCCURRENCE																
	A Frequent	B Reasonably Probable	C Remote	D Extremely Remote	E Extremely Improbable												
I CATASTROPHIC Collision, Fatality, System Loss, Severe Damage	IA R1	IB	IC R2	ID	IE												
II CRITICAL NMAC, Severe Injury, Severe Illness, Major System Damage, Service Termination	IIA	IIB	IIC R3	IID	IIE R4												
III MARGINAL Loss of Separation, Minor Injury, Minor Illness, Minor System Damage, Loss of Comm (single aircraft), Service Interruption	IIIA	IIIB	IIIC	IIID	IIIE												
IV NEGLIGIBLE Less Than Minor Injury or Illness, Less Than Minor System Damage	IVA R4	IVB	IVC	IVD R5	IVE												
<table><tr><th><u>Risk Assessment Code</u></th><th><u>Criteria</u></th></tr><tr><td>R1</td><td>Risk must be eliminated or controlled to an acceptable level. Residual risk is extremely high, and additional mitigation will be required.</td></tr><tr><td>R2</td><td>Risk is still considered very high because of the nature of Alaska operations. Risk must be controlled to an acceptable level.</td></tr><tr><td>R3</td><td>Risk is considered moderate.</td></tr><tr><td>R4</td><td>Risk is considered low.</td></tr><tr><td>R5</td><td>Risk is considered very low.</td></tr></table>						<u>Risk Assessment Code</u>	<u>Criteria</u>	R1	Risk must be eliminated or controlled to an acceptable level. Residual risk is extremely high, and additional mitigation will be required.	R2	Risk is still considered very high because of the nature of Alaska operations. Risk must be controlled to an acceptable level.	R3	Risk is considered moderate.	R4	Risk is considered low.	R5	Risk is considered very low.
<u>Risk Assessment Code</u>	<u>Criteria</u>																
R1	Risk must be eliminated or controlled to an acceptable level. Residual risk is extremely high, and additional mitigation will be required.																
R2	Risk is still considered very high because of the nature of Alaska operations. Risk must be controlled to an acceptable level.																
R3	Risk is considered moderate.																
R4	Risk is considered low.																
R5	Risk is considered very low.																

Figure D-7: ADS-B Capstone Radar-Like Services Risk Matrix [130].

While the function performed for ADS-B is as a surveillance source to air traffic control, the scope of hazards was not limited to this function. Examples include hazard with associated risks of ground impact, loss of pilot situation awareness, and inappropriate use of ADS-B displays for cockpit-based separation [130].

The safety assessment process used was to decompose the evaluation of risk and required mitigations by hazard. This is illustrated in an example scenario shown in Table D-3. The scenario involves collision of an aircraft using ADS-B with terrain or a fixed object. The scenario was selected because it is one of eight scenarios with the highest risk measure. There were no scenarios with a risk ranking of R1, and no air traffic-control related scenarios with a

risk ranking of R2. Thus, the scenario illustrates both a high risk, and a risk outside of the scope of radar services.

Table D-3: Example Hazard Assessment for Capstone ADS-B-Based Separation [130]

Scenario #	Scenario Description	Possible Effect	Risk	R#	Recommendations for Precautions, Controls, and Mitigation
9	Two ADS-B aircraft on approach IFR. Inadvertent loss of voice communication occurs to single aircraft due to environmental effects.	Loss of voice communication single aircraft Slight increase in controller workload.	IIIE	R4	<p>8. ADS-B radar-like separation standard (e.g., 5 nmi, MEAs) is defined to allow intervention time for ATC and pilot to respond safely in case of system failure or other contingencies.</p> <p>9. MFD could enhance pilot situational awareness in the event of a ground system and/or avionics failure.</p> <p>17. Avionics certification, installation, and approval process in place for Capstone, in conformance with standard certification procedures (e.g., TSO-129C, DO-178B (software) and AC-23.1309-1C (hardware)). STC will be amended for ADS-B radarlike services.</p> <p>25b. Pilot ability to see-and-avoid in VMC.</p> <p>27. Standard pilot and controller procedures (e.g., AIM and 7110.65) for lost voice communications will be applied when using ADS-B as a surveillance source, the same as when using radar beacon system as a surveillance source.</p> <p>29 Air-to-air ADS-B traffic depiction can provide an additional means of detection of ADS-B aircraft</p> <p>30. The avionics have been tested, per procedures defined in RTCA/DO-160D, to environmental categories as listed in the various Capstone avionics installation manuals.</p>

In the assessment of the hazard, system elements judged to influence the risk and their associated numbers above were: airspace procedures: separation standards (8) and ATC/pilot common procedures (27); avionics: multi-function display MFD functionality (9), certification (17), testing (30) and traffic information (29); pilot see & avoid procedures (25b). Thus, the system elements are distributed across a range of airborne and ground systems. Some safety-derived requirements already exist in the system, such as defined safety separation standards, while others are required to be performed before system implementation, such as avionics certification and testing.

The actual measures of influence assessed are unknown, as further rationale is not provided on the effectiveness of controls in mitigations in each area, but it can be inferred that all components had some degree of influence. Based on this influence, a qualitative mental model was used to judge the associated risk level.

Reassessment of ADS-B to Radar Separation

The implementation of ADS-B based separation in Capstone included displays to controllers for separation both between ADS-B returns, and ADS-B and radar returns. In February 2007, the office of Air Traffic Oversight (AOV) expressed concerns that the Safety Risk Management Document used as the basis for this implementation did not adequately address potential risks of ADS-B/radar separation. For this reason, approval for the practice was removed and re-assessment was required [136]. AOV had specific concerns about the lack of scope of hazards related to boundaries of radar coverage, and the influence of terrain.

As a result, the application for ADS-B to radar separation was resubmitted after reassessing ADS-B to radar risks. The assessment addressed the scope concerns addressed by AOV, and separation procedures of ADS-B to radar traffic were reinstated [137].

D.7.2 Discussion

The initial hazard assessment for ADS-B radar services was heavily focused on aircraft-based hazards. This is likely the cause of the failure to include sufficient conditions within the scope of analysis for approval of ADS-B to radar separation. However, the justification for initial implementation of ADS-B to radar separation was unavailable in the review of the case. The process of disapproval, and re-approval of this procedure indicates the challenges associated with adequately scoping analysis.

D.8 U.S. Deployment of Automatic Dependent Surveillance Broadcast (ADS-B)

D.8.1 Overview of ADS-B Performance Parameters

ADS-B can utilize different sources for navigation information with different levels of accuracy. To account for this, standards developed for ADS-B define key parameters used to encode the position accuracy and integrity. Three of these parameters will be discussed here. The Navigation Integrity Category (NIC) indicates the position uncertainty boundary to a given level of probability (typically 10^{-7} events/hr). The probability is defined in the Surveillance Integrity Level (SIL). Accuracy of position is defined to a 95% confidence level, and is encoded in the Navigation Accuracy Category for position (NAC_p). It should be noted that previous versions of ADS-B combine integrity and accuracy into a single parameter, the Navigation Uncertainty Category (NUC), but the focus of this discussion is on later versions that separate integrity and accuracy.

There are specific mappings of each parameter to boundaries on position or probabilities. Accuracy and Integrity values are shown in Table D-4 for reference. Surveillance Integrity Levels are shown in Table D-5.

Table D-4: Relationship of NIC/NAC Codes to Position Uncertainty (adapted from [125])

Nav. Integrity Category (NIC)	Containment Radius (R_c), < and Vert. (VPL, <)	Nav. Accuracy Category (NAC)	Horizontal Accuracy Bound (EPU, 95% <)	Vert. Acc. Bound (VEPU, 95%, <)	Equiv. Accuracy
0	unknown	0	> 10 nm		
1	20 nm	1	< 10 nm		RNP-10
2	8 nm	2	4 nm		RNP-4
3	4 nm	3	2 nm		RNP-2
4	2 nm	4	1 nm		RNP-1
5	1 nm	5	0.5 nm (926 m)		RNP-0.5
6	0.6 nm (1111 m) 0.5 nm (926 m)	6	0.3 nm (557 m)		RNP-0.3
7	0.2 nm (370 m)	7	0.1 nm (185 m)		RNP-0.1
8	0.1 nm (185 m)	8	0.05 nm (92.6 m)		GPS (SA on)
9	75 m, VPL – 112 m	9	30 m	45 m	GPS (SA off)
10	25 m, VPL – 37.5 m	10	10 m	15 m	WAAS
11	7.5 m – VPL – 11 m	11	3 m	4 m	LAAS

Table D-5: Definition of SIL Codes (adapted from [125])

Surveillance Integrity Level (SIL)	Probability of Exceeding R_c without detection
0	unknown
1	1×10^{-3} per flight hour or per operation
2	1×10^{-5} per flight hour or per operation
3	1×10^{-7} per flight hour or per operation

D.8.2 Comparison of ADS-B Application Performance Requirements

As part of the program approval requirements for Segment 1 of ADS-B deployment in the U.S. National Airspace System, a Preliminary Hazard Analysis (PHA) was conducted [131]. The PHA uses a risk matrix approach. The details of the Segment 1 PHA will not be covered in this discussion. It is useful to note that as part of the mitigation of midair collision risks in the PHA, a requirement was derived to conduct a probabilistic analysis to identify the required performance for mixed ADS-B/radar separation.

Interviews conducted indicated that this analysis uses two approaches [102]. The first approach is assessment to a target level of safety. The second approach is in comparison of equivalent

performance to a reference system. Thus, the overall safety case for ADS-B relies on the utilization of all three approaches discussed in this work.

In addition to safety assessments conducted for the U.S. program, several other studies have been conducted to determine required performance for potential future applications. Potential future applications assessed by RTCA [134] along with requirements in U.S. and EU [138] policy are shown in Table D-6. The six applications assessed by RTCA are: ASSA, FAROA, EVAcq, ACM, ASIA, and ICSPA. Detailed descriptions of each application are included in the reference and are consistent with their titles [134].

In general, the requirements for each application were derived from the combination of safety assessments and operational performance analysis conducted independently for each application. Integrity requirements are derived through a safety assessment using fault tree or failure modes and effects analysis. Accuracy requirements are based on a structured assessment of the required performance within the operational environment.

Table D-6: Accuracy and Integrity Parameters Required for Selected Applications

Application	Minimum Navigation Parameter Required			Reference
	NACp	NIC	SIL	
Airport Surface Situation Awareness (ASSA)	9	9	1 (10-3)	[134]
Final Approach Runway Occupancy Awareness (FAROA)	9	9	1	[134]
Enhanced Visual Approach (EVApp)	7	8	1	[134]
Airborne Conflict Management (ACM)	N/A	7	2	[134]
Approach Spacing for Instrument Approaches (ASIA)	8	9	2	[134]
Independent Closely-Spaced Parallel Approaches (ICSPA)	9	9	2	[134]
ATC Surveillance in Non-Radar Areas (NRA)	5	4	2	[139]
<i>ADS-B Out for Air Traffic Control</i> ¹²	9	7	2	[140]

¹² The NPRM does not relate specified requirements to individual applications. Strictly speaking, this is not an application.

As can be noted, the requirements for airport awareness applications are higher than those for airborne surveillance. This is due to the increased accuracy required to discriminate position relative to fixed objects and other vehicles on the airport surface. As airborne separations are generally higher, there is a lower level of required accuracy and integrity.

In addition, performance requirements in radar airspace are generally higher than non-radar applications. This is due to the latency associated with radar sweeps compared to ADS-B position reports. When two aircraft are in close proximity, radar illuminates each aircraft at nearly the same time, reducing the position error associated with the travel of the aircraft between position reports. In some operational scenarios, the probability of reception of an ADS-B message results in substantial latency between radar sweeps and the ADS-B report. Thus, the baseline required position uncertainty of the ADS-B system is required to be higher to compensate for the travel latency [141]. In non-radar environments, this latency does not exist. Although there is still potential for latency between ADS-B reports, it is typically lower than a full radar sweep.

D.8.3 Interaction of ADS-B with TCAS

TCAS is certified to issue advisories and alerts under a complex set of conditions based on the computation of a time to closest point of approach. These conditions result in an envelope of protection for which the TCAS system has been certified as safe. If a proposed change involves operating within the TCAS envelope, TCAS will be a significant interacting element, as pilot reactions to traffic alerts and resolution advisories will influence the occurrence of proximity-related risks in the proposed change. In addition, within the envelope, the interaction of the proposed change and TCAS can result in an increase in false alerts to the pilot. This can reduce trust in TCAS alerts, reduce TCAS effectiveness in other operational conditions, and interfere with the desired operation.

Several ADS-B applications will potentially conflict with TCAS due to reductions in planned separation. Studies are currently underway to consider the potential next step in the evolution of TCAS, which may include higher fidelity surveillance and the incorporation of trajectory information from other aircraft. These changes should continue to enable flexibility in collision avoidance logic, to allow for the incorporation of new operations.

D.8.4 Discussion

The wide variation in performance requirements by application creates a tension in setting required performance. The requirements from the NPRM have been placed based on expected future application requirements for high accuracy and integrity [140], although it can be noted that the integrity requirement is not sufficient to meet the required performance for some ground-based applications. The EU has placed lower requirements on initial installations for non-radar areas [138]. This illustrates a fundamental tension in balancing requirements for expected versus current applications.

An additional challenge in ADS-B is due to the long time scale of development of standards. Underlying standards for equipment have gone through several revisions. An example is the minimum Operational Performance Standard (MOPS) for 1090 Mhz Extended Squitter (1090ES) [142]. Early avionics based on the DO-260 standard allowed for the use of either of two potential measures of position uncertainty. During later revisions, only one of these measures was determined to be acceptable for use in air traffic control (ATC) separation. As a result, the installation of ADS-B avionics in individual aircraft must be modified to use the approved method of broadcasting position uncertainty. As an example, Airservices Australia currently has to certify each individual airframe before the aircraft could utilize ADS-B for ATC separation [143]. The DO-260 specification has been changed once, the current DO-260 Change 1. The second version of the 1090 ES MOPS, DO-260A, has been changed three times, with the current version published as DO-260A Change 3.

The uncertainty in required standards can create a disincentive for operators to equip, and can discourage early adoption.

D.9 Unmanned Aircraft Systems (UAS)

D.9.1 Overview and System Description

An Unmanned Aircraft System (UAS) is composed of single or multiple unmanned aerial vehicles, a ground station, and command and control infrastructure. Unmanned aircraft are usually equipped with sensors, such as electro-optical and infrared cameras, which typically provide information relayed to the ground station or other customers. There are several other potential applications for UAS, as the aircraft exist along a broad spectrum of capabilities in terms of size, payload, endurance, and ceiling [144].

Unmanned aircraft have been historically operated by the military. Recently, there has been an increased need for access to civil airspace, for border surveillance missions, military training flights, and manufacturer testing of aircraft. There is also a desire to utilize UAS for civilian, academic, and law enforcement applications.

Current aviation regulations did not anticipate operation without a pilot onboard, and several aspects of UAS challenge the basis for current approval processes and flight rules. This has led to several global efforts to accommodate UAS in civil airspace, a current review is provided in [145]. In the United States, FAA Unmanned Aircraft Systems Program Office [146] was formed to develop interim guidance and approval processes for limited introductions of UAS [146]. RTCA is also developing standards for UAS equipment.

A key limitation is a lack of inherent ability of an onboard pilot to detect and avoid potential conflicts with other aircraft operating in airspace. Current regulations require that “vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft [147].” Translating this requirement to unmanned aircraft has led to the need to evaluate traffic detection technologies or procedures that replace this functionality of an onboard pilot. For UAS, this capability is known as Detect, Sense and Avoid (DSA).

The following discussion of the UAS case will be organized slightly differently due to the nature of the pending change. The first two sections of this case will focus on determination of required performance of DSA systems to meet safety acceptability criteria. This discussion will begin

with the early establishment of criteria and interim standards for the DSA function. Following this, current efforts are underway to perform a structured safety assessment of UAS DSA will be described.

UAS also present other significant challenges in operational approval due to the fundamentally new type of operation they represent. UAS operations present changes in pilot roles, changes in task allocation between pilots and automation, and changes in potential risks and associated severity of risks. These challenges in evaluating fundamentally new operations will be discussed in the third section.

D.9.2 Detect Sense and Avoid Functionality

Early standards developed by ASTM. ASTM developed one of the first standards for UAS sense and avoid sensor performance in 2004 [148]. The standard describes performance-based requirements for a DSA sensor in terms of field of regard, range, and resolution. In the process of developing the ASTM standard, two safety assessment approaches were used. The first was an equivalent performance approach, which based sensor performance on the equivalent field of regard and detection capabilities of the human eye. Through analysis of several midair collision scenarios, it was found that human detection performance was insufficient to resolve a significant number of potential collisions, and direct performance comparison was therefore not used as a basis for deriving UAS sensor performance [149].

Instead of equivalent performance, a TLS approach was then used to design system performance. Near midair collision (NMAC) rates for general aviation were estimated based on an estimated ratio of NMACs given midair collisions, and an analysis of midair collision rates reported by the FAA. This yielded an average NMAC rate of 8.6×10^{-6} / hr. The target rate was used to derive sensor range, field of regard, and resolution requirements using a Department of Defense modeling tool [149].

To date, the ASTM standard has not been accepted by the FAA as an acceptable means of compliance with DSA requirements. It is likely due to the implicit rejection of pilot see and avoid performance as an acceptable reference system, both in terms of a safety target, and in visual acquisition performance. Additionally, the target is nearly two orders of magnitude less

safe than 1×10^{-7} requirement in the ATO SMS for a hazardous severity of risk for which an NMAC would be ranked.

Interim Equivalence Approaches to DSA. Current U.S. operations of UAS are approved by the FAA Unmanned Aircraft Systems Program Office (UAS PO). The program office combines multiple areas of expertise in air traffic procedures, and airworthiness certification. The UAS PO has published interim guidance on operational approval of UAS operations. There are two mechanisms by which UAS operations can be approved: experimental aircraft certification, or through a Certificate of Authorization (COA). Both require examination of individual operations, site visits, and significant operational restrictions [146].

As interim policy, the standards are not required to go through the full safety assessment and rulemaking process as other regulations. For this reason, a combination of expert judgment and best practices were used to derive the guidance. A basis was still necessary to determine requirements to see and avoid other aircraft, as the risk severity is potentially catastrophic. For this reason, an equivalence approach was used.

One equivalence approach is to segregate UAS operations to restricted airspace, which eliminates the DSA function. This is similar to current restricted airspace practices used to protect non-military aircraft from encounters potentially more dangerous military aircraft or missile operations.

Two interim approaches to performing DSA also utilize equivalence. These are the use of a chase aircraft, and the use of ground observers. A chase aircraft that flies in formation with the UAS and acts as a surrogate in communication with air traffic control. The pilot of the chase aircraft is responsible for detection and avoidance of other aircraft. This directly replaces the function an onboard pilot would perform, and seeks to remove any variation that would change levels of risk associated with the see and avoid task, as well as the task of communicating with air traffic control.

A second approach recognized as acceptable by the FAA is to utilize ground observers. Ground observers are generally required to be spaced no more than 1nm laterally and 3,000 ft vertically from the UAV [146]. The aircraft can only operate within visual contact with the ground

observers at all times. The lateral distance is the same VFR weather minimums for low visibility conditions, set at 1 nm, indicating an assumed limit on pilot/observer detection capability.

By the ground observer approach, the task that an onboard pilot would perform in visual conditions has been directly transferred to ground-based personnel. This introduces other variations in performance that were not explicitly considered. Ground observers have different reference frames than an onboard pilot would, which can influence the ability to identify resolution maneuvers. Ground observers must also communicate with the UAS remotely, introducing a potential failure path in execution. Regardless of these differences, the approaches are attractive because they are equivalent in function to current methods of performing the task.

The basis for using equivalence for current UAS DSA standards seems to conflict with the rejection of equivalence in the ASTM standard. While the details are not directly documented, differences in the approach can be identified that explain the apparent conflict.

The ASTM standard proposed set functional performance as a standard for technology. It is likely that this process bears increased scrutiny than internal FAA policy judgments. The performance of general aviation aircraft sense and avoid, as a reference system for deriving a technical standard, was not acceptable. However, the same functional role in a human, in the specific cases evaluated by the UAS PO was judged to be acceptable. This judgment could indicate that UAS observers would perform better than average pilots of the reference system. It could also indicate implicitly higher process standards for the derivation of technical requirements.

RTCA DSA MOPS development. The ASTM standards development approach has been de-emphasized by the FAA. Instead, the FAA has tasked RTCA Special Committee 203 (SC-203) with developing Minimum Operational Performance Standards (MOPS) for detect, sense, and avoid and command and control systems [150]. RTCA has traditionally developed system requirements in an advisory role to the FAA, as noted in the ADS-B case study above.

Although the results are not complete, RTCA is using a risk matrix approach to assess and mitigate hazards related to the use of each system [151]. The practice in development of MOPS

is to use safety assessment as the basis for deriving some aspects of system performance, with others driven by other requirements.

D.9.3 Challenges Due to Fundamentally New Operational Capability

UAS DSA as a Fundamentally New Capability. The significant change in task allocation for performance of traffic avoidance represents a fundamentally new operational capability. The sense and avoid task has been performed by onboard pilots, and assured through training and pilot certification. In UAS, the task is transferred to onboard equipment, potentially with a pilot in the loop. The transfer of functionality from a pilot to equipment fundamentally changes the approval path for DSA equipment. Instead of being assured through pilot certification, approval must be obtained for DSA avionics and software, and new operational procedures approved for flight crews operating the system.

Deriving equipment standards requires examination of several additional system elements that influence associated risks. These can include the characteristics of surrounding traffic, DSA sensor performance, collision avoidance or alerting logic, and resolution actions. Potential hazards associated with each function must also be assessed within the scope of analysis.

In changing task allocation, it becomes less possible to qualify performance by similarity. A suitable technical system does not exist to use as a reference system or to qualify by similarity. System behavior also becomes more difficult to decompose in the same way similarity can be used to determine required radar performance. The entire control process is coupled, such that tradeoffs are evaluated between, for example, sensor performance and conflict identification. There is also the ability to improve upon current human-based sense and avoid practices.

The performance requirements derived from the safety assessment are expected to be demanding. By the judgment of the FAA associated administrator for aviation safety, feasible technology to perform detect, sense, and avoid to an acceptable level of safety is currently not available and not likely to be available in the near future [152]. There is a risk that technical performance requirements could be demanding such that suitable technology cannot be developed to meet the performance requirements.

Changes to Severity Classifications. As described in Section 3.3, severity rankings associated with a potential risk are defined based example descriptions of harm associated with the risk. Implicit in severity definitions is a presumed shared fate between the flight crew and occupants on an aircraft, and the general public on the ground. In addition, embedded in the current definitions of severity are indicators of increased risk, as discussed in Section 5.1.2.

UAS operations change the events used to define associated severity levels. Instead of potentially harmful effects to occupants and crew of the aircraft, there is the addition of potential harms to third parties on the ground. One study [153] has addressed harms to the public by incorporating fatal injuries to third parties into severity definitions. The study also addressed unique failure modes as indicators of increased risk, such as loss of communication and associated control of the vehicle as a catastrophic event, regardless of the harm it may pose directly to individuals [153].

Elimination of Shared Fate between Flight Crew and UAS. By removing the flight crew and occupants from the UAS, there is removal of “shared fate” between the operators of the UAS and the UAS itself. There is a perception that this may adversely influence the safety decision-making priorities of operators. Under hazardous conditions, operators may be less likely to take extraordinary measures to prevent harms if direct harm to operators is not a consequence. If this is the case, current operational procedures and flight crew certification may be judged to be less effective at mitigating risks. Thus, the new operational nature challenges assumptions under current approaches and may require re-evaluation or special consideration before operational approval.

Removal of Flight Crew from Direct Control of Aircraft. While in most modern aircraft flight crew commands are processed through a fly-by-wire system, remote operation of UAS removes flight crew even further from direct control. This can remove sensory inputs regarding vibration, smell, and sound that could indicate hazardous conditions [154]. This reduces the ability to compare similar tasks between traditional flight crews and UAS operators.

In addition, the introduction of a communications link can pose additional risks. Latencies and failure conditions introduced by the link require a new approach to mitigating risks than in a traditional aircraft. The potential for loss of control also results in the incorporation of some

autonomous behavior in most UAS. The onboard autonomy often functions to execute aircraft control in the advent of a loss of communication with the ground either to re-establish link, or safely terminate the flight of the UAS. Onboard autonomy and the presence of a communications link can expand the necessary scope of safety assessment to additional risks, and the additional associated elements.

D.9.4 Discussion

The fundamentally new nature of UAS operations has had implications for several safety assessment and operational approval decisions. Because of the lack of regulatory guidance directly applicable to UAS and the lack of a full safety assessment, interim standards have been based on judgment, and a substitution to equivalent performance. This approach has enabled limited operations, but it is not comprehensive or rigorous enough to support routine operations.

Recognizing two driving equipment requirements for command and control and detect sense and avoid, efforts through RTCA have begun to develop equipment standards to be used as the basis for certification. These have limited scope by decomposing two functions that are of concern in UAS operation. Even with the decomposition, there is still a significant scope of analysis required to derive required performance for acceptable safety. Additionally, there is a risk that the performance required in DSA and command and control systems may be specified to a level that is unachievable with available technology, or prove costly to implement by the majority of desired operators.

Beyond command and control and detect, sense and avoid, there will be a substantial set of analyses required to determine the safety acceptability of UAS operations. Changes in pilot tasks, levels of autonomy, and severity of risks are a few areas that drive a large scope of analysis required.

It should be noted that the current approaches to evaluating UAS safety do not include airspace design within the scope of analysis. The burden of mitigation lies within elements of the UAS system. With the exception of limited use of restricted airspace to segregate UAS operations, the requirement to change airspace structure has not been evaluated. In this way, the current requirements of airspace limit achievable performance of unmanned aircraft.