



NLR Air Transport Safety Institute

Research & Consultancy

NLR-TP-2012-439

DEVELOPMENT OF A REGULATORY SAFETY BASELINE FOR UAS SENSE AND AVOID

A. Oztekin
R. Wever



Executive summary

DEVELOPMENT OF A REGULATORY SAFETY BASELINE FOR UAS SENSE AND AVOID

Problem area

Unmanned Aircraft Systems (UAS) emerge as a viable, operational technology for potential civil and commercial applications in the National Airspace System (NAS). Although this new type of technology presents great potential, it also introduces a need for an analysis of its safety impact on the NAS. On-going efforts to develop rules and requirements for UAS Sense and Avoid (SAA) underlines the need to understand to what extent existing regulations cover the related hazards. The objective of this study is to develop and apply a generic methodology to identify risk controls that the current regulations provide to mitigate the hazards and causal factors in a certain domain, new operation or technology.

Description of work

This study presents a systems-level approach to analyse the safety impact of introducing a new technology and to determine a regulatory baseline. Within the context of this study, a system-level perspective refers to looking at the air transport

system as a whole from a high-level of abstraction as a system.

The proposed methodology is applied to the (near) mid-air collision under IFR (Instrument Flight Rules) operations. First, a set of hazards and underlying causal factors for (near) mid-air collision risk is determined based on a causal risk model. Next, the associated regulatory risk controls are determined by a review of a selected set of aviation rules and regulations by means of subject matter experts.

Results and conclusions

This study presents a methodology that can be used to define a minimum set of risk controls based on current rules and regulations to control or mitigate hazards related to a certain operation or new technology. The methodology is applied to the domain of mid-air collision and the resulting baseline is comprised of three hazards with 60 underlying causal factors, and a large number of applicable regulatory risk controls. The analysis of the risk controls indicates to what extent the current regulations

Report no.

NLR-TP-2012-439

Author(s)

A. Oztekin
R. Wever

Report classification

UNCLASSIFIED

Date

December 2012

Knowledge area(s)

Vliegveiligheid (safety & security)

Descriptor(s)

UAS
safety
see and avoid

The contents of this report have been initially prepared for publication as article in the Handbook of Unmanned Aerial Vehicles by Springer.

act as risk controls for hazards associated with mid-air collision in the NAS. This provides an understanding of potential gaps in the existing regulatory structure, by identifying the hazards and underlying causal factors for which current regulations provide potentially no or limited mitigation.

The results show that some hazards and causal factors are well covered by multiple rules/regulations. On the other hand the study demonstrates that with this approach one is able to identify possible gaps in regulations to control the risk of certain hazards. The resulting set of risk controls is not only applicable to manned operations in the NAS but will also provide a minimum, but possibly not sufficient, set of risk controls to mitigate (near) mid-air collision risk for UAS operations.

The value of the presented approach lies in the structured analysis to identify the existing

regulatory coverage for the hazards present in a certain domain. In particular, the methodology supports the analysis regarding the extent to which identified hazards for a particular domain are covered by existing regulations. Thus, the proposed approach facilitates the identification of gaps in the current regulations for a specific risk or domain.

Applicability

The developed generic methodology could be applied to a new technology or operation to identify hazards and corresponding regulatory risk controls on a system-level. It is applied to mid-air collision domain, but that could easily be extended to cover other areas of interest, such as command, control, and communication for UAS integration into the NAS. As such, this study contributes to development of standards for safe integration of UAS in non-segregated airspace.

NLR-TP-2012-439

DEVELOPMENT OF A REGULATORY SAFETY BASELINE FOR UAS SENSE AND AVOID

A. Oztekin¹
R. Wever


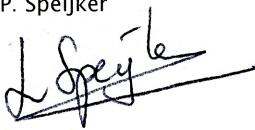

¹ Hi-Tec Systems, Inc., FAA William J. Hughes Technical Center

The contents of this report have been initially prepared for publication as article in the Handbook of Unmanned Aerial Vehicles by Springer.

The contents of this report may be cited on condition that full credit is given to NLR and the author(s).

Customer	Ministry of Transport, Public Works and Water Management
Contract number	-----
Owner	NLR
Division	Air Transport
Distribution	Unlimited
Classification of title	Unclassified December 2012

Approved by:

Author R. Wever 	Reviewer L.J.P. Speijker 	Managing department A.D.J. Rutten 
Date: 11/12/2012	Date: 11/12/2012	Date: 11-12-2012

This page is intentionally left blank.

Development of a Regulatory Safety Baseline for UAS Sense and Avoid

66

Ahmet Oztekin and Rombout Wever

Contents

66.1	Introduction	2
66.2	Defining a Safety Baseline	3
66.3	Challenge with the UAS	4
66.4	Regulatory-based Causal Factor Framework	5
66.5	Approach to Construction of a Safety Baseline for SAA	7
66.6	Causal Model for Midair Collision.....	9
66.7	Approach to Identifying Regulatory Risk Controls for SAA	12
66.8	Analysis of Regulatory Risk Controls	15
66.9	Concluding Remarks.....	21
	References	22

Abstract

Unmanned Aircraft Systems (UAS) emerge as a viable, operational technology for potential civil and commercial applications in the National Airspace System (NAS). Although this new type of technology presents great potential, it also introduces a need for a thorough inquiry into its safety impact on the NAS. This study presents a systems-level approach to analyze the safety impact of introducing a new technology, such as UAS, into the NAS. Utilizing Safety Management Systems (SMS) principles and the existing regulatory structure, it outlines a methodology to determine a regulatory safety baseline for a specific area of interest regarding a new aviation technology, such as UAS Sense and Avoid. The proposed methodology is then employed to determine a baseline set

A. Oztekin (✉)

Hi-Tec Systems, Inc., FAA William J. Hughes Technical Center, Atlantic City International Airport, 08405, Atlantic City, NJ, USA
e-mail: ahmet.ctr.oztekin@faa.gov

R. Wever

NLR Air Transport Safety Institute (NLR-ATSI), Amsterdam, The Netherlands
e-mail: Rombout.Weaver@nlr-atsi.nl

of hazards and causal factors for the UAS Sense and Avoid problem domain and associated regulatory risk controls.

66.1 Introduction

Unmanned Aircraft Systems (UAS) present great potential for civil and commercial applications in non-segregated airspace. Unrestricted UAS access into the National Airspace System (NAS) of the United States requires a thorough examination of its safety impact on the current operations in the NAS. In addition, a lack of regulatory guidance is considered an obstacle against achieving the full potential that UAS has to offer (FAA Flight Plan 2009–2013; Weibela and Hansman 2005). Recognizing the need for regulations and guidance material, aviation regulators initiated efforts to develop policies and establish requirements, procedures, and standards that will support UAS technology development and certification to enable safe operations of UAS. In the United States, Federal Aviation Administration (FAA) is working closely with the UAS community through RTCA Special Committee 203 (SC-203) to define the Minimum Aviation System Performance Standards (MASPS). Similarly, EUROCAE Working Group 73 (WG-73) is coordinating European efforts to deliver standards and guidance that will ensure the safety and reliability of unmanned aircraft missions operating in non-segregated airspace (EUROCAE 2009). These efforts are also being informally coordinated to facilitate harmonization (RTCA 2010).

The integration of UAS into the NAS presents various unique challenges, which will require novel and mostly platform-specific technological solutions. However, it can be argued that demonstration of airworthiness of these technologies will not present the only barrier to the introduction of UAS in the NAS. The difficulty that UAS is currently facing arises in obtaining authorization to enter and use civil airspace. This originates from the legitimate concern that unmanned aircraft may collide with other aircraft. Given the consensus that there will be no dedicated airspace for UAS operations, some authorities place the primary role of avoiding any collision between UAS and manned aircraft solely to the UAS. For all practical purposes, the UAS is, therefore, expected to have full responsibility to sense other aircraft and take effective evasive action. In this context, “see and avoid” or “sense and avoid” (SAA) emerges as one of the areas, which introduces new challenges and technologies compared to manned aviation and raises attention of regulators as well as the UAS manufacturers and future operators.

The body of current research projects on sense and avoid in the UAS domain mainly focuses on technology development and demonstration to provide a portfolio of workable technological solutions for the see and avoid concept. As compared to technology development, research on UAS safety risk analysis with an emphasis on SAA is still in its infancy. Most current UAS safety studies perform the risk analysis at a very detailed level based, on limited event or occurrence data. Examples of such research are preliminary functional hazard assessments (Hayhurst et al. 2007), event-based safety models of UAS (Weibel 2005), and simulation-based

encounter models (Kochenderfer et al. 2008). However, a systems-level safety analysis focusing on the regulatory aspects of the SAA concept for UAS operations with an emphasis on future NAS access is lacking.

This study outlines a systems-level safety risk analysis framework for the SAA concept. Within the context of this study, a system-level perspective refers to looking at the air transport system as a whole from a high-level of abstraction as a system, or a system of subsystems. Thus, NAS may be considered as the system and UAS as a subsystem. In particular, the proposed framework presents a novel regulatory-based and integrated approach to understand hazards associated with midair collision risk and SAA and provides an analysis of current regulatory controls related to this topic. Utilizing Safety Management Systems (SMS) principles, the proposed framework establishes a systems-level safety analysis approach based on the FAA regulatory requirements to support the safe integration of UAS into the NAS with a particular focus on “sense and avoid.” The framework is intended to provide insight in risks and risk controls in current regulations when integrating new and complex technologies into the NAS while meeting the FAA’s SMS mandates. This study divides potential operations in the NAS into two main subgroups: flights conducted under Visual Flight Rules (VFR) and Instrument Flight Rules (IFR). The analysis and results presented here were developed for IFR operations.

In this study, the terms “hazard” and “causal factor” are used within the following context: A hazard is a condition, object, or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function. Hazards occur usually due to several causal factors. In general, hazards are considered at a higher level of abstraction, whereas causal factors are of a more detailed level.

The research presented here is based on the concepts and ideas that have been introduced in (Luxhøj et al. 2009, 2010; Oztekin and Luxhøj 2008, 2009). The next section provides background information on these concepts that are instrumental to the analysis, results, and discussion presented. Consequently, the proposed approach is illustrated by using a causal model for midair collision as the basis to develop a safety baseline for the SAA concept. Finally, an analysis on the SAA safety baseline is presented along with some concluding remarks.

66.2 Defining a Safety Baseline

In order to regulate a new technology that is to operate within an already-established and well-regulated infrastructure, such as NAS, without risking stifling its potential, one needs to understand existing safety criteria required to achieve the level of safety associated with the current operations. Within the context of the NAS, the existing safety criteria are the applicable aviation rules and regulations governing everyday manned flight and flight support and management operations of commercial or noncommercial nature. In this context, aviation rules and regulations act as controls against potential risks and provide a baseline for safe operations in the NAS.

More specifically, regulations are risk controls that constitute a safety baseline for all operations in the NAS. All aircraft operating in the NAS have to satisfy requirements set by Title 14 Code of Federal Aviation Regulations (14 CFR) and follow supporting guidance material. 14 CFR provides the risk controls for safe operations and establishes a baseline for all prospective operation in the NAS. For UAS technology and operations in nonsegregated airspace, current regulations (14CFR) apply. Thus, understanding the risk controls as defined by 14 CFR and outlining a baseline set of hazards and underlying causal factors that existing regulations control lie at the crux of the regulatory safety baseline concept (Oztekin and Lee 2011; Oztekin et al. 2011).

66.3 Challenge with the UAS

Limited availability of data on emergent nature of UAS operations introduces a challenge for the safety analysis and assessment of UAS operations. Conventional quantitative safety risk analysis techniques, essentially event-driven and largely built upon past experience and vast amount of historical data, may not provide adequate information for risk controls necessary for emerging technologies such as UAS. In the absence of operational data, it becomes very difficult to perform a systems-level safety analysis of UAS using conventional quantitative safety analysis methodologies. However, this situation can be considered as typical for any new technology with a limited accumulation of historic operational data. In this context, it is argued that a new approach may add valuable insight to understand the safety impact of emerging UAS operations on NAS. This new approach should not rely on historic data about the new technology, therefore would not be hindered by the lack of it. Furthermore, it should also assume a systems-level perspective while performing the safety analysis. Thus, a successful attempt to understand the safety impact of emerging UAS operations of civil/commercial nature can be achieved through a higher systems-level approach, which takes into account the problem domain as a whole. In this case, the problem domain in question is the NAS and it should be treated as a single complex system. Subsystems, such as Air Traffic Control (ATC), Airmen, Aircraft, Flight Operations, and Airspace constituting the NAS are interdependent and their interactions determine safety that permeates the whole system and defines minimum mandatory safety requirements for the NAS. These minimum set of requirements constitute a mandatory baseline for conducting safe operations in the NAS. A systematic approach for the identification of such a safety baseline will provide guidance to understand systems-level safety impact of a new technology, such as UAS, onto the NAS. Utilizing the safety baseline concept, Regulatory-based Causal Factor Framework (RCFF) (Luxhøj et al. 2009, 2010; Oztekin and Luxhøj 2008, 2009; Oztekin and Lee 2011; Oztekin et al. 2011, 2012), provides such a systematic approach. Although RCFF is a new and intuitive approach, one should make it clear that it does not replace but complements existing qualitative and quantitative methods by recognizing existing rules and regulations

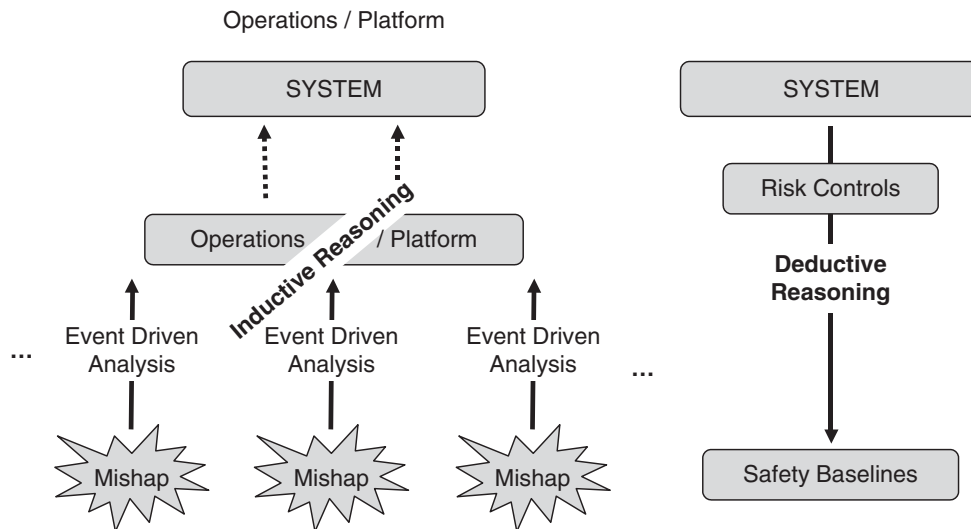


Fig. 66.1 Inductive reasoning versus deductive reasoning

covering the problem domain as key components of a system-level qualitative safety risk analysis framework.

Data-centric methodologies benefit from *inductive reasoning* when modeling the problem domain and the system in question. Although inductive reasoning has been successfully employed for data-rich systems for which extensive collections of case studies exist, due to similar reasoning outlined above, inductive frameworks may not be a good fit to understand and model new technology with limited accident/incident data. In this context, this study adopts *deductive reasoning* to understand the problem. [Figure 66.1](#) illustrates deductive approach as compared to inductive reasoning. Deductive reasoning is a top-down approach, which puts emphasis on modeling the system based on its higher and more general components. When applied to the area of safety analysis, contrary to inductive approach where the analysis would be based on individual accident/incident cases and related data, a deductive approach will study the system as a whole and focus on its higher-level components and their interactions. Thus, a deductive approach will concentrate on understanding the safety minimums and, using an engineering term, determine the boundary conditions for conducting safe operations within the system.

66.4 Regulatory-based Causal Factor Framework

The study presented in this chapter utilizes concepts introduced by the RCFF. In very broad terms, RCFF is a qualitative, systems-level approach to safety assessment based on deductive reasoning to construct a safety baseline for operations in the NAS in the United States. The basic concept relies on two fundamental premises: Aviation rules and regulations “Title 14 Code of Federal Regulations (14 CFR)”

provide minimum mandatory requirements (i.e., risk controls) for safe operations in the NAS and various unrelated regulations interact to provide risk controls for hazards.

14 CFR can be considered as the culmination of efforts by the larger aviation community to provide an inherent minimum level of safety for every single operation to be conducted within the NAS. This notion of minimum safety is outlined as rules and requirements by the 14 CFR, and every aircraft in the NAS has to operate above the minimums of this mandatory safety baseline. In this sense, regulations act as minimum controls for potential risks associated with operating in the NAS.

However, individual regulations do not operate in a vacuum. When a specific aircraft or operation is concerned, a diverse collection of rules regulating different areas of the NAS interact to provide minimum requirements for safety as they apply to the specifics of the operation/aircraft in question. For example, issues related to certification of aircraft, aircraft engine, or propeller are regulated by 14 CFR Part 21, whereas airworthiness standards for the aircraft and its components are outlined in Parts 21–33. Subchapter D of 14 CFR focuses on the issues of certification and training of airmen and Subchapter E defines and partitions airspace, within which the proposed operation is set to take place. Thus, every single operation in the NAS, whether that particular type of operation has been conducted routinely for many years or it is the implementation of a new technology, is enveloped by a mandatory minimum safety baseline created collectively by various interacting rules regulating potential sources of various different hazards.

The notion of interactions between various parts of the 14 CFR to provide a minimum mandatory safety risk controls is a simple yet powerful idea, which brings forth a new approach to understand and study safety in aviation. This intuitive idea, in fact, borrows from the fundamental principle of the interdisciplinary field Systems Analysis. Formally, systems analysis is the dissection of a system into its component pieces for purposes of studying how those component pieces interact. In complex systems such as NAS, safety is the product of these interactions. However, a closer look at various current research efforts on UAS integration in the NAS reveals that such studies rarely explore potential interactions between their respective area of interest and various other components of the NAS, in a systematic fashion.

The regulatory-based approach of RCFF takes cues from FAA's own Safety Management System (SMS) process. FAA Policy Document on SMS Guidance (FAA 2008) states that

...regulations will serve as risk control, if correctly applied in the context of the unique operational environments of service providers. Rule making process therefore should apply the concepts of safety risk management ...They [regulations] should identify hazards ... Compliance with the regulations would thus move beyond viewing them on as administrative requirements and into an environment where compliance entails effective control of clearly identified hazards. This would enhance the value of regulations as effective instruments of safety management. Regulations and subsequent oversight activities must be part of a strategy of risk control.

This understanding of regulation’s role coincides with the fundamental concepts that RCFF is built upon; namely, use regulations as risk controls, identify hazards based on risk controls, identify causal factors underlying hazards, determine potential interactions between causal factors (thus between risk controls). Within the context outlined in the FAA SMS Guidance, RCFF can also be used as part of an exploratory risk-based rule-making process as a future research initiative, where the impact of the current regulations as risk controls are evaluated on the safety baseline and shortcomings are identified and corrected.

RCFF adopts a deductive, top-down approach to identify systems-level hazards and associated causal factors using regulations (i.e., 14 CFR) as risk controls. This approach is especially a good fit for providing a system-level qualitative safety risk analysis of emerging technologies, such as UAS, where limited availability of case data poses a challenge. RCFF also proposes a methodology to determine connections between potentially related causal factors, thereby creating an interlinked safety baseline. Ultimately, the RCFF safety baseline can be explored to understand the interactions between causal factors, as well as the dependencies between regulations (i.e., risk controls).

The outcome of the RCFF process is the safety baseline: hazards, causal factors, and regulations as risk controls. The context and scope of the safety baseline is determined by the set of regulations included in the RCFF analysis. Hazards and causal factors are identified based on risk controls outlined by these regulations. The scope of an RCFF analysis and the extent of the resulting safety baseline can be adjusted both depth-wise and breadth-wise in terms of detail and coverage.

Conceptually, the RCFF hierarchy closely follows the current regulatory structure. At the very top of this hierarchy, covering the entire NAS, Federal Aviation Regulations (14 CFR) provide minimum risk controls for safe operations. Thus, an RCFF top-down modeling process starts with regulations, or rather, it accepts regulations as input. However, risk controls can also be found beyond 14CFR: orders, technical manuals, guidance material, even prior safety studies are among the source materials that can be used as risk controls to initiate the process for an RCFF-based analysis.

The RCFF hierarchy including risk controls, hazards, causal factors, and linkages between them are stored in a database. A detailed discussion on the methodology used to construct an RCFF hierarchy based on the existing set of regulations and to populate the RCFF database is provided in Oztekin and Lee (2011) as part of a proof-of-concept study, where a potential utilization of the database is outlined. The high-level implementation of RCFF utilizes 14 CFR Parts as the basis to develop its hierarchy and the resulting system-level safety baseline (Oztekin and Lee 2011).

66.5 Approach to Construction of a Safety Baseline for SAA

Current regulations prescribe generic risk controls against midair collision and near midair collision risk. Under provisions that regulate operations near other aircraft, FAR Sect. 91.111 (b) states that “no person may operate an aircraft so close to

another aircraft as to create a collision hazard.” Additionally, FAR Sect. 91.113 (b) quoted below, explicitly uses language that includes the terms “see and avoid” and “well clear”: “When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear.” Obviously, the need for UAS to comply with the SAA concept in the NAS extends well beyond these two 14 CFR sections and a more detailed analysis of regulations with a particular emphasis on current risk controls for hazards related to (near) midair collision is needed.

See and Avoid can be used to assure separation from other aircraft and to avoid collisions in case separation failed. The SAA concept can be divided into two areas, namely, separation assurance and collision avoidance (Lacher et al. 2008). Separation assurance covers topics ranging from airspace structure and procedures to onboard alert systems such Traffic Collision Avoidance System (TCAS). On the other hand, collision avoidance entails the act of sensing and avoiding traffic conflicts or executing the collision avoidance maneuver once all preceding protective layers fail to provide the separation required. Most of the UAS SAA-related research focus on technology development that falls within the domain of collision avoidance. When it comes to understanding the safety impact of various interacting components of the NAS on the UAS SAA, there is more to it than sensor technology and algorithm development. Therefore a more integrated approach is needed to conduct a safety analysis of UAS SAA.

The objective of this study is to define a safety baseline for (near) midair collisions and the SAA concept. In this study, the RCFE concept has been applied to identify risk controls that the current regulations provide to mitigate the hazards and causal factors related with (near) midair collisions and the SAA concept. The result is a set of risk controls derived from existing regulations that will not only be applicable to manned operations in the NAS but will also provide a minimum, but possibly not sufficient set of risk controls to mitigate (near) midair collision risk for potential UAS operations. Operations conducted under instrument flight rules (IFR) and visual flight rules (VFR) have to be considered to develop a minimum mandatory baseline for SAA which applies to a wide range of traffic encounters under all operational environments. The current study is focused on IFR operations only.

In this context, the study presented in this chapter is composed of the following three phases:

1. Identify a baseline set of hazards and underlying causal factors for (near) midair collisions and the SAA concept. A causal model developed and validated specifically for this topic is used as the starting point to identify a baseline set of regulatory risk controls.
2. Identify risk controls for the causal factors. The risk controls are derived from existing regulations. The risk controls along with the hazards and causal factors constitute the safety baseline for preventing (near) midair collisions;

3. Perform an analysis of existing regulatory controls. The objective of the analysis is to quantify and understand the coverage that the identified regulatory risk controls provide to potentially mitigate the hazards and causal factors associated with the SAA safety baseline. Such an analysis also focuses on interactions between different domains of regulatory controls and helps to determine the coverage or gaps in regulatory material concerning regulating the new system, operation, etc.

Since the RCFE exists conceptually and not yet as a full-scale application, it is not possible to apply RCFE directly to the SAA concept, as the set of associated causal factors, hazards, and risk controls is not available yet. Instead, a detailed causal model developed specifically for the issue at hand provided a good starting point to identify a set of hazards and causal factors and associated regulatory controls that could form the safety baseline for the midair collision risk and SAA concept.

Considering that RCFE is a top-down framework, this “bottom-up” approach may seem inconsistent. However, the basic idea behind the RCFE is that regulations provide a set of risk controls for hazards (and causal factors); these regulations interact and their interactions can be identified through identifying dependencies between hazards (or between causal factors). The ultimate goal of RCFE is to determine risk controls and their interactions for the problem domain in question. Using existing knowledge about hazards and causal factors (i.e., a causal model) to identify the regulatory risk controls and their dependencies is still consistent with the RCFE concept.

66.6 Causal Model for Midair Collision

A causal model explains the functional and quantitative relationship between the various factors affecting risk in the Air Transport System (or NAS) or major parts of it. Generally speaking, such models allow the user to understand how, and how much, changes in a particular part of the ATS change the local as well as the overall safety risk of the ATS.

The hazards and causal factors in relation to (near) midair collision and SAA for IFR operations were identified by means of an existing causal model, which was developed as part of the Causal Model for Air Transport Safety (CATS) study (Ale et al. 2005; CATS 2008). The CATS study was a major effort sponsored by the Dutch government and developed by a consortium of parties including the NLR-Air Transport Safety Institute. The aim of CATS was to understand the causal factors underlying the risks of commercial air transport. It is an integrated quantitative causal model that can be used for safety risk analysis and assessment in civil air transport. The backbone of CATS consists of 33 generic accident scenarios. Each accident scenario was modeled as an Event Sequence Diagram (ESD), a flowchart which starts with an initiating event and progresses through pivotal event toward a set of possible outcomes (e.g., accident, incident, and continued flight). Each path through the flowchart is a scenario. Along each path, pivotal events are identified as

either occurring or not occurring. Fault Trees connect to the events in the ESD and represent the deeper, underlying causes of these events.

The causal model is composed of a qualitative as well as a quantitative part. The qualitative part is formed by the ESD and Fault Tree structure defining the accident scenario and causal pathways leading to different outcomes. In other words, event names and descriptions and the relationships between events, the model structure, constitute the qualitative model. The model was quantified using accident, incident, and occurrence data as well as expert judgments. It is crucial to maintain the context of the ESD and Fault Trees and avoid drastically revising language and model structure; otherwise the quantified model elements would no longer be valid.

This study utilizes (near) midair collision ((N)MAC) as the system-level hazard to define the SAA problem domain. (N)MAC as an event has been fully studied to understand underlying hazards and causal factors using available occurrence data from aviation safety databases. Analysis indicated that the SAA problem domain in the NAS can be decomposed into two main operational sub-domains, namely, operations conducted under instrument flight rules (IFR) and under visual flight rules (VFR). All potential scenarios need to be studied to fully cover the problem domain and develop a minimum mandatory baseline for SAA which applies to all encounters under all operational environments. The resulting safety baseline for SAA will not only be applicable to manned operations in the NAS but will also provide a minimum, but possibly not sufficient, set of risk controls to govern potential UAS-specific hazards.

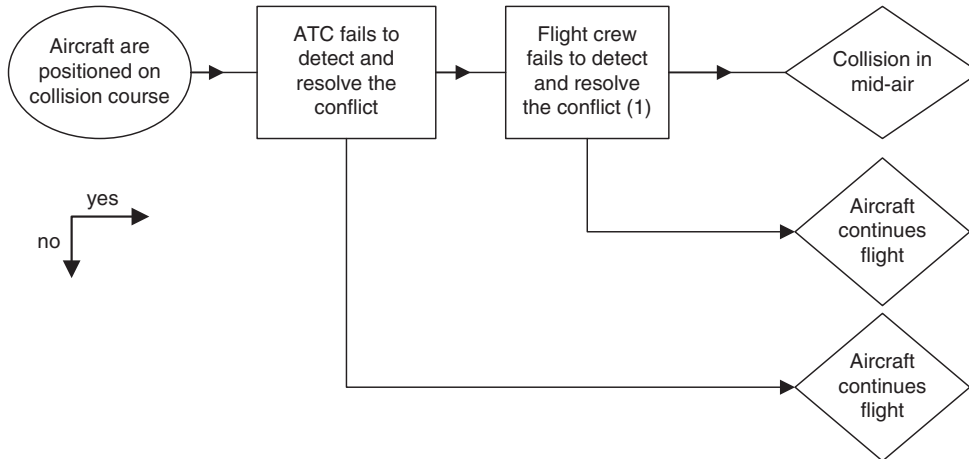
In this context, the study presented here is based on the MAC/NMAC encounters involving two aircraft-operated under IFR, thereby partially covering the operational domain of the NAS, as the current scope of this research.

The ESD for midair collision is one of the 33 generic accident scenarios modeled in CATS and describes generically hazards and causal factors in relation to (near) midair collision and SAA for IFR operations. The initiating event is “aircraft are positioned on collision course” and the end states are “collision in midair” or “aircraft continues flight.” The detailed specific or possible causes or contributing factors of the pivotal events in the ESD are added by Fault Trees underneath each pivotal event. The ESD models two layers of conflict detection and resolution: ATC and the flight crew (supported by, e.g., collision avoidance systems and SAA). The models were developed by a combination of retrospective and prospective analysis. The retrospective analysis consisted of a detailed and structured analysis of aviation accidents, which demonstrate typical accident patterns. The prospective analysis is based on engineering knowledge and aviation operational domain experts to identify potential hazards and hazardous combinations of causal factors that may have not (yet) resulted in an accident.

The ESD is representative for Part 121 operations with Part 25 aircraft and entails the encounter of two aircraft operating under IFR. It is composed of the initiating event and two pivotal events, and together with the associated Fault Trees, it has 29 intermediate events and 61 base events, see [Fig. 66.2](#).

The ESD for midair collision is used as the basis to develop a minimum mandatory safety baseline for SAA. However since the scope of the midair collision

Accident type: mid-air collision.
 Flight phases: initial climb, en-route and approach.
 Initiating event: aircraft are positioned on collision course.



(1) This pivotal event includes the execution of ‘see-and-avoid’ principle and the response to a Traffic Collision Avoidance System alert.

Fig. 66.2 Event sequence diagram used to develop the components of the SAA safety baseline

model is limited to IFR, only the portion of the SAA safety baseline that covers IFR operations within the NAS is modeled by the study presented here.

The events constituting the Fault Tree supporting the ESD were originally defined using short descriptive texts which outline the intended scope of the event within the context of the accident scenario in question. The causal model elements were reviewed by a group of subject matter experts (SMEs) to identify causal factors and hazards that will constitute the safety baseline for SAA in the NAS. During the course of the review process, the original language used to describe the events was also revised by the SMEs so as to fit the terminology currently prevalent in the NAS. The review process resulted in 3 “system-level” hazards and 60 causal factors constituting the SAA safety baseline for IFR operations in the NAS.

The set of hazards and causal factors are generic and applicable to both manned and unmanned aviation operations. Some causal factors may have a minor different interpretation in case of unmanned aircraft, without affecting the cause-effect relationship. For example, some causal factors may refer to “pilot” which can be interpreted as “UAS operator” without changing its cause-effect relationship. However, the identified set of causal factors should be reviewed in more detail to identify potential missing causal factors related to UAS-specific operations and technology.

The original causal model for midair collision is composed of a qualitative as well as a quantitative part. The qualitative part is comprised of the ESD and Fault Tree structure defining the accident scenario and causal pathways leading to different outcomes. In other words, event names and descriptions and how they

are placed in the model structure constitute the qualitative model. The model was quantified using accident, incident, and occurrence data as well as expert judgments. Thus, the causal model for midair collision, as a whole, represents a certain probability distribution. However, if it becomes necessary to include additional UAS-specific hazards as part of a future study, associated Fault Trees may also need to be revised quantitatively resulting in a new probability distribution representing the revised causal model.

66.7 Approach to Identifying Regulatory Risk Controls for SAA

Once a baseline set of hazards and causal factors was determined from the causal model, the next step was the identification of existing regulations that provide potential controls to prevent and mitigate hazards and causal factors related to midair collision and SAA for IFR operations in the NAS.

The SAA safety baseline presents a simple hierarchical structure. The regulation that explicitly mentions SAA as a safety requirement for conducting operations in the NAS (i.e., FAR Sect. 91.113-b) is at the very top of this hierarchy. Hazards identified for SAA branch out from Sect. 91.113(b), and individual causal factors are listed for each hazard. In this context, risk controls for hazards are identified through individual causal factors. In other words, risk controls are identified for individual causal factors, thus their connections to hazards are indicated through causal factors. Regulations (i.e., 14 CFR) also present a hierarchical structure. Fourteen CFR is grouped into subchapters. Subchapters are partitioned into Parts and Parts into subparts. Subparts are divided into sections. Specificity of information that a regulation provides increases as one moves toward the next lower level in the regulatory hierarchy. Since the safety baseline is comprised of a collection of very detailed causal factors, pertaining risk controls should also present a level of detail that is comparable with the information content of the safety baseline. Thus, for each causal factor, specific 14 CFR sections were identified as potential risk controls. Notional representation of the SAA safety baseline hierarchy based on the structure of the NMAC ESD is illustrated in [Fig. 66.3](#).

Due to resource constraints, this study limited the scope of the risk control identification to 13 FAR Parts representing three major subchapters of 14 CFR as sources for potential risk controls. The FAR Parts and corresponding subchapters included in this study are listed below:

Subchapter C – Aircraft:

Part 21 – Certification Procedures for Products and Parts

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

Part 25 – Airworthiness Standards: Transport Category Airplanes

Part 27 – Airworthiness Standards: Normal Category Rotorcraft

Part 33 – Airworthiness Standards: Aircraft Engines

Part 34 – Fuel Venting and Exhaust Emission Requirements for Turbine Engine Powered Airplanes

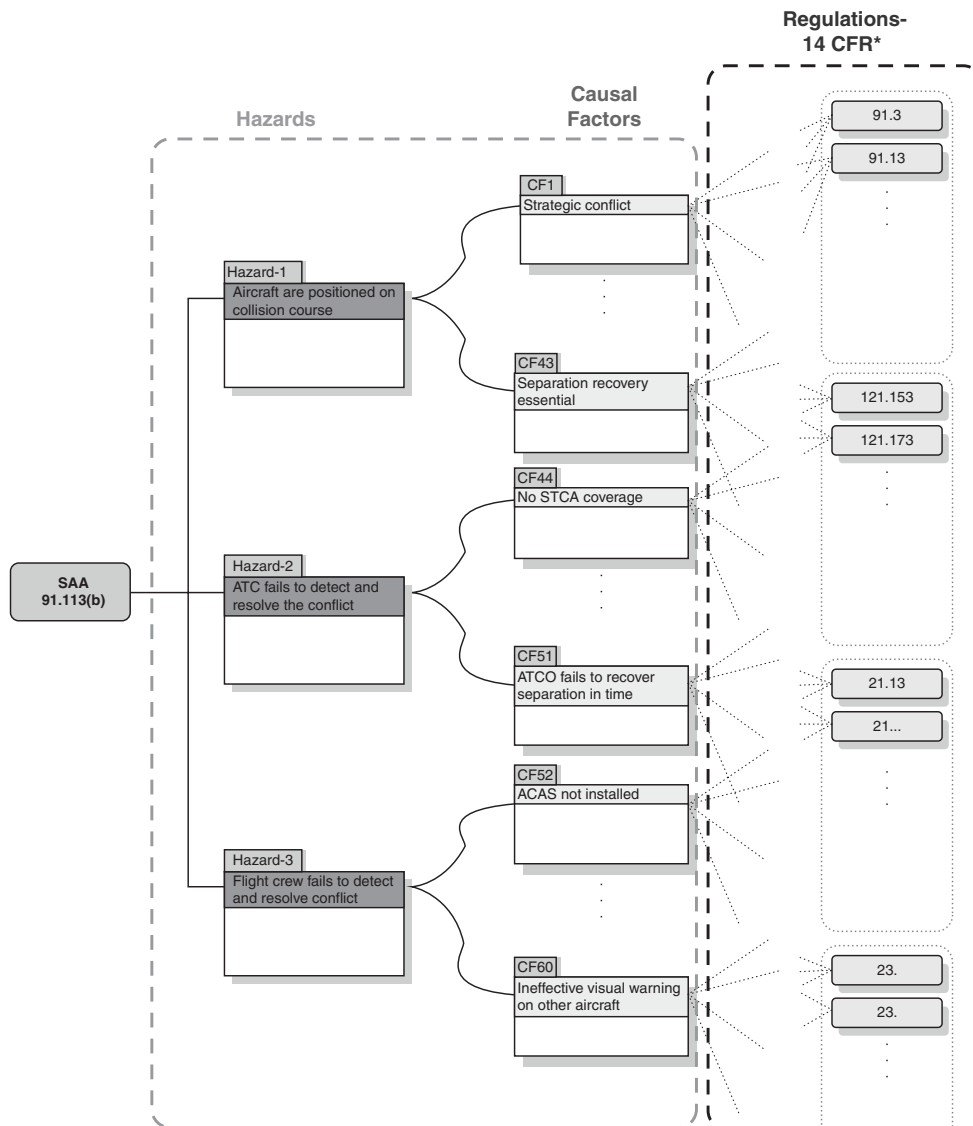


Fig. 66.3 Notional illustration of the SAA safety baseline

Part 43 – Maintenance, Preventive Maintenance, Rebuilding, And Alteration

Subchapter D – Airmen:

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

Part 65 – Certification: Airmen Other Than Flight Crewmembers

Subchapter F – Air Traffic and General Operations:

Part 91 – General Operating and Flight Rules

Subchapter G – Air Carriers and Operators for Compensation or Hire: Certification and Operations:

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
Subchapter H – Schools and Other Certificated Agencies:
Part 145 – Repair Stations

Note that the Parts listed above are some of the most prominent rules regulating aviation safety. Thus they provide extensive coverage in terms of risk controls for the NAS.

The process of identifying section-level risk controls for the identified hazards and causal factors involved multiple knowledge elicitation sessions with Subject Matter Experts (SMEs), with extensive background and expertise on aviation-related rulemaking, regulatory oversight, as well as operations. The sessions were moderated in a structured manner with the participation of multiple SMEs and an aggregate approach was employed to determine potential risk controls for individual causal factors across the 13 FAR Parts mentioned before. The data sample provided below in [Table 66.1](#) illustrates the type and content of the data that has been compiled as the result of the elicitation process to identify risk controls for the SAA safety baseline.

Table 66.1 Risk controls identified for CFs #4 and #5 of Hazard #1. Only risk controls from Parts 65, 91, 121, and 135 are shown

Hazard #1							
Aircraft are positioned on collision course							
			Risk controls				
#	Causal factor	Definition	Part 91	Part 135	Part 65	Part 121	Part 61
4	Inadequate strategic surveillance picture	The radar picture is inadequate to allow the Planning Controller to identify the pre-tactical conflict, e.g., incomplete traffic picture, picture with overlapping labels, or too much traffic for the display system	N/A	135.18	N/A	121.357, 121.356, 121.360	N/A
5	Inadequate flight plan data	Flight plan data is inadequate to allow the Planning Controller to identify the pre-tactical conflict, e.g., incorrect flight plan, flight plan insufficient to identify conflicts, flight plan strips obtained too late, or aircraft not following flight plan	91.173, 91.111, 91.113, 91.123	135.345, 135.347	65.31, 65.33, 65.35, 65.37, 65.39, 65.45, 65.49, 65.50	121.395	61.87, 61.93

66.8 Analysis of Regulatory Risk Controls

This section presents the analysis of risk controls that were identified according to the methodology outlined above. First, the identified risk controls are analyzed from a higher systems-level perspective and its interaction with the NAS as a whole. Next, individual causal factors are analyzed to achieve a more in-depth understanding of the SAA safety baseline and its interaction with the NAS.

The reader should bear in mind that the scope of this study includes only the 13 FAR Parts listed in the preceding section and this fact should be taken into consideration when reviewing the result presented here. Even though a set of regulations were identified in this study as applicable risk controls for a certain hazard or causal factor, there is still a need for further analysis to determine the extent to which these controls mitigate the risks associated with that hazard.

Potential system-level hazard sources underlying midair collision can be analyzed according to the Hazard Classification and Analysis System (HCAS) (Oztekin and Luxhøj 2008; Luxhøj et al. 2009, 2010). HCAS identifies four system-level hazard sources, namely, Aircraft, Operations, Airmen, and Environment, whose interactions impact any potential hazards within the context of the NAS. These system-level hazard sources are also in line with the 14 CFR subchapters.

The causal factors identified in the SAA safety baseline can be allocated to these four system-level hazard sources. Likewise the risk controls derived from the review of 13 FAR Parts can be categorized under the four main categories of interest: Aircraft, Airmen, Operations, and Certification. The distribution of risk controls over those categories is shown in Fig. 66.4 for the SAA safety baseline (IFR case only).

Note that Fig. 66.4 indicates a distribution over the total count of risk controls identified according to the methodology outlined in this chapter. Thus, 31 % of the risk controls identified originates from Part 91 corresponding to Air Traffic Control and General Operations Rules. Risk controls from Operational Certification–related Parts, namely, Parts 121 and 135, also provide 31 % of all the risk controls identified.

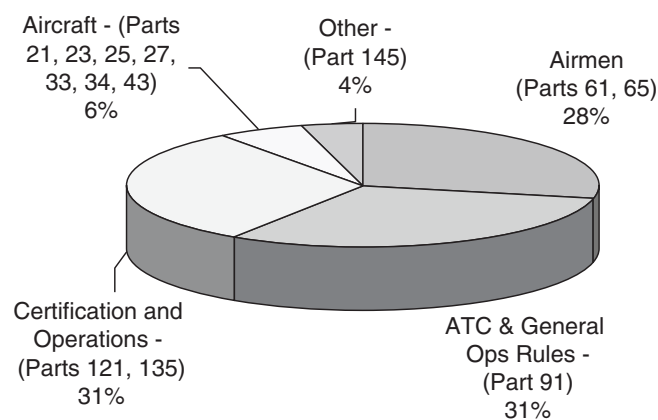


Fig. 66.4 Distribution of risk controls for the SAA safety baseline according to the four major categories of interest (IFR only)

While 28 % of the risk controls are Airmen related, only 6 % can be attributed to Aircraft certification–related regulations. Thus, one can conclude that, for the SAA safety baseline, existing rules regulating operational aspects of the NAS provide the majority of controls, whereas only a minority of the controls originate from current regulations governing aircraft certification. However, one should bear in mind that the analysis presented throughout this chapter is based only on the 13 Parts included in this study.

The SAA safety baseline includes three system-level hazards, namely, Loss of Separation, Failure by ATC, and Failure by Flight Crew. The hazard “Loss of Separation” represents the case that two aircraft are on a collision course/lost separation. The hazard “Failure by ATC” depicts a situation where, given that loss of separation occurs, ATC fails to detect and resolve the conflict. The hazard “Failure by Flight Crew” refers to a case where, given that Loss of Separation and Failure by ATC have occurred, the flight crew fails to detect and resolve the conflict. The distribution of risk controls identified for these three hazards over the categories Aircraft, Airmen, Operations, and Certification are shown in Figs. 66.5–66.7, respectively.

The system-level hazard “Loss of Separation” contains 43 causal factors for which 11 separate FAR Parts provide risk controls. Figure 66.5 indicates that 36 % of the risk controls for Loss of Separation are provided by sections of Part 91, which provides ATC and general operations rules for the NAS. Operation certification–related Parts (i.e., Parts 121 and 135) and Airmen-related Parts (61 and 65) each provide 26 % of the risk controls for Loss of Separation respectively. Considering how closely the hazard is associated with operational and ATC-related issues, this sort of a distribution is to be expected. Regulations such as Parts 21, 23, and 25 that govern aircraft and component certification provide a small portion of the risk controls (7 %) for the identified hazards/causal factors.

The system-level hazard “Failure by ATC” has eight causal factors. Three separate FAR Parts provide risk controls as shown in Fig. 66.6. Half of the risk controls are provided by Parts 61 and 65, whereas 44 % of the controls come from

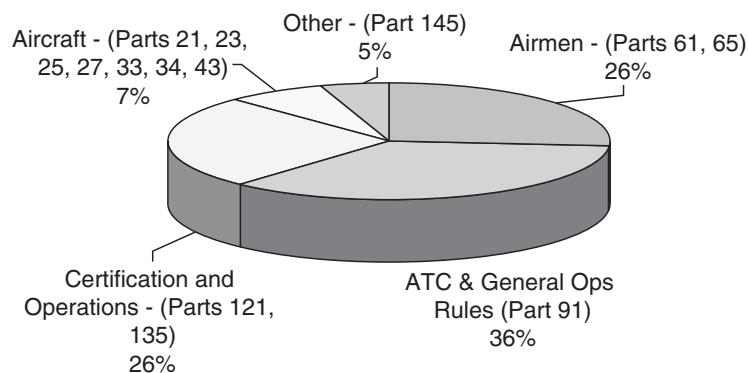


Fig. 66.5 Distribution of risk controls for the system-level hazard loss of separation

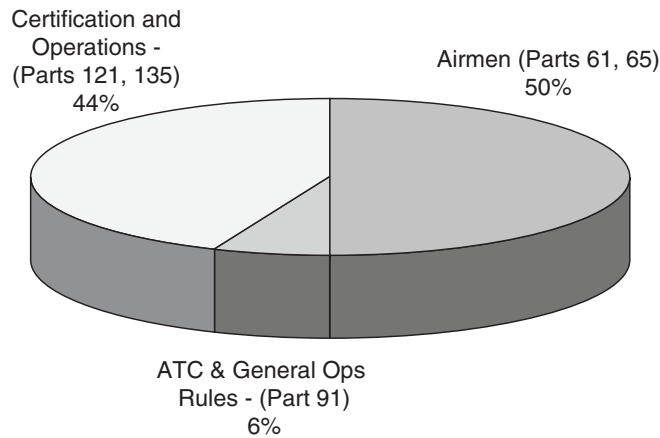


Fig. 66.6 Distribution of risk controls for the system-level hazard failure by ATC

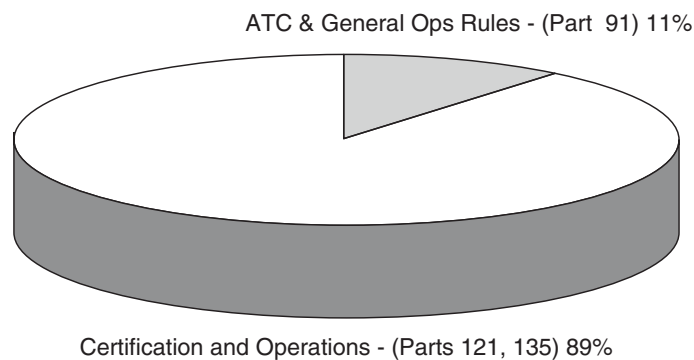


Fig. 66.7 Distribution of risk controls for the hazard failure by flight crew

operation certification–related regulations. Only 6 % of the controls originate from Part 91.

Figure 66.7 presents the distribution of the risk controls for the third and the last system-level hazard constituting the safety baseline: Failure by Flight Crew. Nine causal factors were identified under this hazard and three FAR Parts provide potential risk controls. Among the 13 FAR Parts included in the scope of this study, only Parts 91, 121, and 135 provide risk controls for the causal factors grouped under this hazard. Operation certification–related regulations, namely, Parts 121 and 135, present the overwhelming majority of the risk controls, whereas Part 91 provides only 11 % of the total controls for this hazard and underlying causal factors.

A more detailed analysis of the risk controls can also be performed at the level of causal factors constituting the SAA safety baseline for the IFR operations. Such an analysis is presented below with a particular emphasis on individual causal factors.

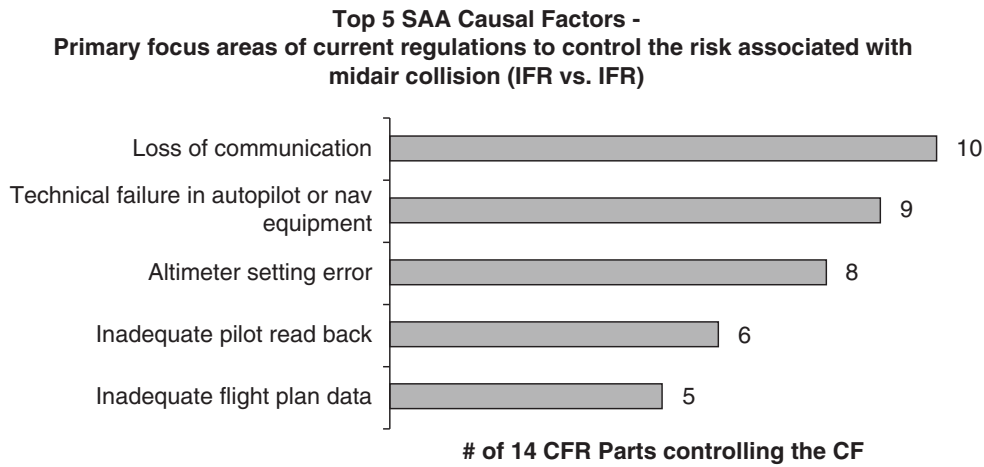


Fig. 66.8 Top causal factors in the SAA safety baseline with the highest number of 14 CFR sections acting as risk controls

Certain causal factors in the safety baseline receive relatively better coverage by 14 CFR sections acting as potential risk controls. The top five causal factors for which existing regulations provide the highest number of risk controls are presented in Fig. 66.8.

The causal factor “Loss of Communication” is defined as “communication between ATC and pilot is lost during a conflict in uncontrolled airspace due to technical failure or human error.” Forty-six regulatory sections are identified as potential risk controls for this factor. A closer look at these risk controls reveals that 10 different FAR Parts out of the 13 investigated by this study provide controls for mitigating or preventing potential risk associated with loss of communication. However, note that even though a set of regulations was identified as applicable risk controls for this causal factor, there is still a need for further analysis to determine that these controls fully mitigate the risks associated with the factor.

The lower end of the coverage spectrum, on the other hand, provides a glimpse of causal factors for which review regulations presents little to no coverage on the identified hazards/causal factors. Table 66.2 shows the causal factors that are potentially covered by only one or no section-level risk control.

Figure 66.7 and Table 66.2 help by illustrating the value of the proposed approach, which provides an analysis regarding to what extent the hazards and causal factors identified for the SAA are covered by existing regulations. Thus, the proposed approach facilitates the identification of gaps in the current regulations for a specific problem domain, in this case for SAA. These gaps indicate areas of potential risk within the SAA baseline, for which current regulations do not provide proper mitigation.

From the study results, the coverage and gaps in the current regulatory structure as potential risk controls for the identified hazards and causal factors related to midair collisions and SAA are presented in Figs. 66.9 and 66.10. Figure 66.9

Table 66.2 SAA safety baseline causal factors with the least coverage in terms of risk controls that existing regulations provide

Causal factor	Description	# of risk controls
Other aircraft effectively invisible	The other aircraft cannot be seen from the cockpit. (other aircraft may not be visible due to glare, weather (rain), obstruction of view by wings, window frame, poor contrast, etc.)	0
Inadequate tactical surveillance picture	The radar picture is inadequate to allow the Tactical Controller to maintain separation in a plannable conflict, e.g., incomplete traffic picture or picture with overlapping labels	0
ATCO failure to recognize conflict	Tactical Controller obtains adequate flight information but fails to recognize the conflict	1
Conflict due to military traffic	Unauthorized penetration of civilian controlled airspace by military traffic	1
Weather induced level bust	Vertical deviation resulting from weather conditions	1
Level bust results in conflict	Given a level bust occurs, the aircraft has separation infringement with another aircraft	1
ACAS avoidance invalidated by other aircraft	ACAS avoidance action is canceled out by incorrect action from the other aircraft	1
Flight crew fail to observe visible aircraft in time	Pilots fail to observe visible aircraft in time to make avoidance action	1
Pilot fails to take avoidance action in time	Pilots fail to make appropriate avoidance action, having observed the other aircraft with sufficient time to take the necessary action	1
Visual avoidance invalidated by other aircraft	Pilot's response is canceled out by opposing maneuver from the other aircraft	1
Ineffective visual warning on other aircraft	Pilots on the conflicting aircraft fail to resolve the conflict using see and avoid techniques, given similar failure on the subject aircraft	1

presents 14 CFR sections that act as potential risk controls for causal factor #16 “loss of communication between ATC and pilot.” Within the hierarchy of the SAA safety baseline, CF16 is associated with Hazard #1 “loss of separation.” A closer inspection of Fig. 66.10 shows that CF16 is controlled by four distinct grouping (i.e., subchapter) of 14 CFR Parts. In other words, to address hazards related to loss of communication between ATC, the applicability of the individual sections covering these four separate domains of interest need to be investigated to demonstrate that a baseline level of safety is achieved regardless of whether the operation is manned or unmanned. Not all the causal factors of the SAA baseline are covered by

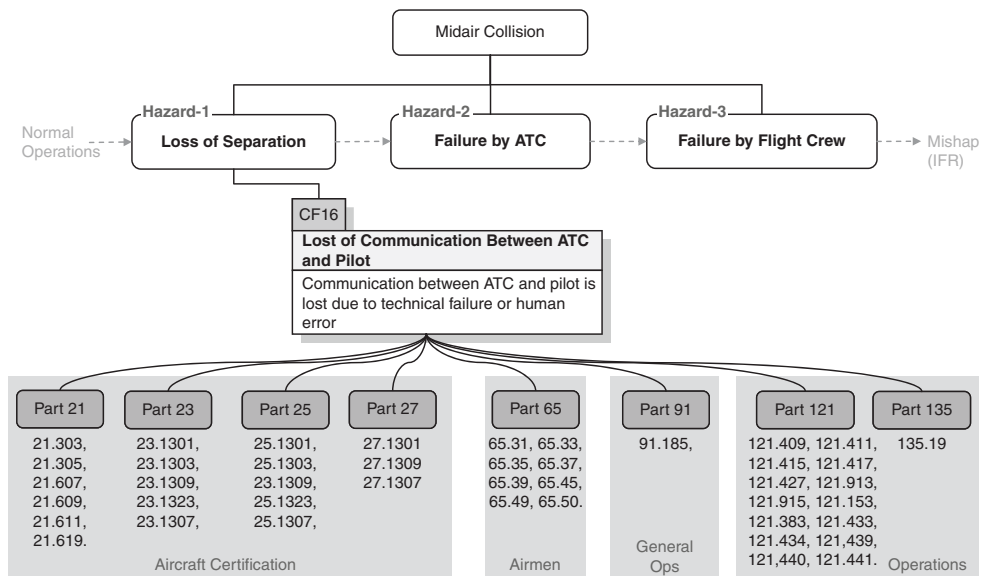


Fig. 66.9 Section level regulatory risk controls identified for CF 16 in the SAA safety baseline

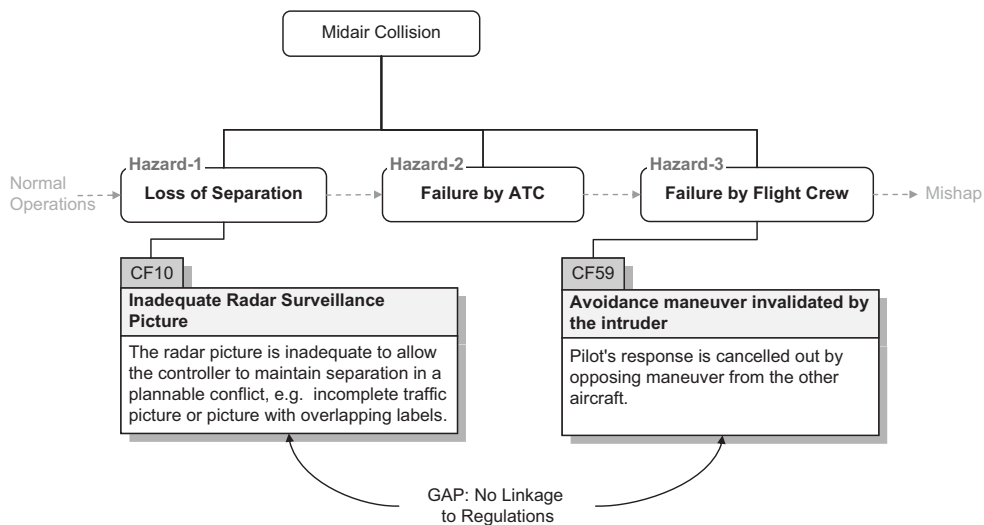


Fig. 66.10 Potential gap in the existing regulations. No risk controls were identified for CF 10 and CF 59 in the SAA safety baseline

an existing regulation acting as risk control, indicating a potential gap in the existing regulatory structure. For example, Fig. 66.10 provides two causal factors in the IFR SAA baseline, for which no regulatory risk controls were identified from within the 13 FAR Parts included in this study.

66.9 Concluding Remarks

Ongoing efforts to develop rules and requirements for UAS SAA underlines the need to understand to what extent existing regulations cover SAA related hazards. In this context, this study presents a methodology that can be used to define a minimum set of risk controls based on current rules and regulations to control or mitigate hazards and causal factors related to a certain operation or technology. The value of the presented approach lies in the structured analysis to identify the existing regulatory coverage for the risks present in a certain domain. In particular, it provides an analysis regarding the extent to which hazards and causal factors identified for that domain are covered by existing regulations. Thus, the proposed approach facilitates the identification of gaps in the current regulations for a specific risk or domain.

The regulatory-based methodology (Regulatory-based Causal Factor Framework, RCGF) was applied to the domain of midair collision and See and Avoid (SAA). The study provided the identification of a set of hazards and underlying causal factors for (near) midair collision and SAA concept based on a causal model. The midair collision scenario was modeled as an Event Sequence Diagram with underlying Fault Trees that further detail the underlying causal factors within the context of IFR-only commercial air transport operations. The causal model provided an initial set of hazards and causal factors for the near midair collision and the SAA concept, which was consequently employed to identify a minimum set of risk controls for the SAA baseline using current rules and regulations.

The resulting SAA safety baseline is comprised of three hazards, 60 underlying causal factors, and a large number of applicable regulatory risk controls. While studying aviation regulations as potential risk controls for the identified hazards and causal factors, an initial set of FAR Parts representative of all major areas of interest in 14 CFR was selected and included in the scope of this study. Risk controls defined in the reviewed set of regulations were identified at the sections level. Finally, a systems-level analysis of risk controls was presented along with a more detailed look at the distributions with respect to the individual hazards and causal factors within the SAA safety baseline.

Although this study concentrates on the SAA problem domain, the proposed approach, coupled with the RCGF concept, is intended to be used for system-level safety analysis and assessment of other core areas of interest such as command, control, and communication for UAS integration into the NAS.

The outcome and the potential value of this study can be surmised as follows:

- It presents a structured approach to determine existing regulatory risk controls in the NAS for hazards related to a specific problem domain, e.g., a new technology. It is argued that the identified risk controls along with the set of hazards constitute a baseline for conducting safe operations within the context of that specific problem domain. This safety baseline establishes potential safety minimums that apply to all current and emergent operations, such as UAS. Consequently, the

safety baseline concept can be used to outline an initial set of safety provisions that apply to the UAS within the context a particular area of interest such as SAA in the NAS.

- It identifies a preliminary set of current risk controls for SAA in the NAS based on a selected group of aviation rules and regulations. The resulting analysis of the risk controls indicates to what extent the current regulations act as risk controls for hazards associated with the SAA in the NAS. This analysis can also be used to provide an understanding of potential gaps in the existing regulatory structure by identifying the hazards and underlying causal factors for which current regulations provide potentially no or limited mitigation. Since it is argued that the same set of risk controls apply to all operations in the NAS, they may also provide a roadmap for outlining safety provisions for the UAS within the context for which the risk controls were identified.

References

- B.J.M. Ale, *Development of Causal Model for Air Transport Safety*, ed. by K. Kolowrocki. Advances in Safety and Reliability ESREL 1 (Taylor and Francis, London, 2005), pp. 37–45
- CATS, The directorate general of civil aviation and maritime affairs, the Netherlands, Causal model for air transport safety, Final Report, May 2008
- Federal Aviation Administration, Safety management system guidance, Washington, DC, Order 8000.369, 30 September, 2008
- Federal Aviation Administration, Flight plan 2009–2013. Washington, DC, http://www.faa.gov/about/plans_reports/media/flight_plan_2009-2013.pdf. Accessed 8 March, 2011
- K.L. Hayhurst, J.M. Maddalon, P.S. Miner, G.N. Szatkowski, M.L. Ulrey, M.P. DeWalt, C.R. Spitzer, Preliminary considerations for classifying hazards of Unmanned Aircraft Systems. Washington, DC, NASA TM-2007-214539, February, 2007
- M.J. Kochenderfer, J.K. Kuchar, L.P. Espindle, J.L. Gertz, Preliminary uncorrelated encounter model of the National Airspace System, Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusetts, Project Report CASSATT-1, ESC-TR-2007-056, 26 June, 2008
- A.R. Lacher, D.R. Maroney, A.D. Zeitlin, Unmanned aircraft collision avoidance: technology assessment and evaluation methods, MITRE Technical Paper, McLean, VA, July 2008. http://66.170.233.9/work/tech_papers/tech_papers_08/07_0095/. Accessed 8 March, 2011
- J. Luxhøj et al., Safety risk analysis of Unmanned Aircraft Systems integration into the National Airspace System: phase 1, Washington, DC, Final Report, DOT/FAA/AR-09/12, September, 2009
- J. Luxhøj et al., Safety risk analysis of Unmanned Aircraft Systems integration into the National Airspace System: phase 2, Washington, DC, Final Report, DOT/FAA/AR-10/12, September, 2010
- A. Oztekin, J.T. Luxhøj, Hazard, safety risk, and uncertainty modeling of the integration of Unmanned Aircraft Systems into the national airspace, in *26th Congress of International Council of the Aeronautical Sciences*, Anchorage, 14–19 September 2008
- A. Oztekin, J.T. Luxhøj, in *A Regulatory-Based Approach to Safety Analysis of Unmanned Aircraft Systems HCI International 2009 Conference Proceedings*. Lecture Notes in Computer Science (LNCS) series (Springer, San Diego, 2009)
- A. Oztekin, C. Flass, X. Lee, S. Keller, Development of a regulatory-based safety analysis framework for Unmanned Aircraft Systems, in *AIAA Unleashing Unmanned Systems Infotech@Aerospace Conference*, St. Louis, AIAA-2011-1418, 29–31 March 2011

- A. Oztekin, C. Flass, X. Lee, Development of a framework to determine a mandatory safety baseline for Unmanned Aircraft Systems. In *J. Intell. Robot. Syst.* **65**(1–4), 3–26 (2012).
10.1007/s10846-011-9578-0
- RTCA, Terms of Reference, Special Committee (SC) 203, Minimum performance standards for Unmanned Aircraft Systems, Washington, DC, Paper No. 065-10/PMC-790, 26 April, 2010
- The European Organization for Civil Aviation Equipment (EUROCAE), Work Group 73 (WG-73): Unmanned Aircraft Systems, Information Compendium, Lucerne, Switzerland, UAS-021.4, 24 April, 2009
- R.E. Weibel, R.J. Hansman, Safety considerations for operation of unmanned aerial vehicles in the National Airspace System, MIT International Center for Air Transportation, Cambridge, Report No. ICAT-2005-1, March 2005