Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-642

Accident Risk Assessment for Advanced Air Traffic Management

H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij and M.B. Klompstra

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2001-642

Accident Risk Assessment for Advanced Air Traffic Management

H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij and M.B. Klompstra

This report is based on an article published in Air Transportation Systems Engineering, Editors G.L. Donohue and A.G. Zellweger, July 2001, Published by the American Institute of Aeronautics and Astronautics, Inc.

Division:	Air Transport
Issued:	December 2001
Classification of title:	Unclassified

Contents

(26 pages in total)

This page is intentionally left blank.

Accident Risk Assessment for Advanced Air Traffic Management

H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams,
M.H.C. Everdij and M.B. Klompstra

National Aerospace Laboratory NLR, Amsterdam, The Netherlands

Abstract

By now, safety is recognised as a key quality on which to select/design advanced air traffic management (ATM) concepts, even when capacity and efficiency are the drivers of the development. The safety target is often described as 'equal or better' in comparison with existing practice, allowing a large freedom in how safety is expressed, let alone measured. In effect, new advanced communication, navigation, surveillance and air traffic management (CNS/ATM) concept developments are typically accomplished without the use of feedback from appropriate safety assessments. ATM concept design teams (e.g., of Free Flight or four dimensional ATM) try to realise capacity-efficiency enhancements by exploiting new technology, changing human controller roles and introducing new procedures, while relying on the established safety-related indicators in ATM such as conflict rates and types, workload of human operators and failure rates and effects of technical systems.

ATM, however, is the result of complex interactions between multiple human operators, procedures and technical systems, all of which are highly distributed. This yields that providing safety is more than making sure that each of the ATM elements function properly safe; it is the complex interaction between them that determines safety. The assessment of isolated indicators falls short in covering the complex interactions between procedures, human operators and technical systems in safety-critical non-nominal situations. To improve this situation, this paper outlines a novel probabilistic risk assessment methodology, which has specifically been developed for application to ATM. In addition, this paper presents risk assessment results which have been obtained with this approach for two en route streams of required navigational performance, 95% of time within 1 n mile (RNP1), equipped traffic flying in opposite direction within two conventional ATM concepts and two airborne separation assurance based concepts. These results illustrate that our new methodology supports safety-based ATM design.

I. Introduction

Air traffic management (ATM) is the result of complex interactions between human operators, procedures, and technical systems (hardware and software), all of which are highly distributed. Providing safety is more than making sure that each of these elements function properly and safely. The complex interactions between the various elements of ATM significantly determine safety. Therefore, it is imperative to understand the safety impact of these interactions, particularly in relation to non-nominal situations. Traditional ATM design approaches tend first to design advanced ATM that provides sufficient capacity, and next to extend the design with safety features. The advantage of this approach is that ATM developments can be organized around the clusters of individual elements, i.e., the communication cluster, the navigation cluster, the surveillance cluster, the automation tools cluster, the human machine interfaces (HMIs), the advanced procedures, etc. The key problem is that safety effects stay unclear. A far more effective approach is to try to design an ATM system that is inherently safe at the capacity-level required. From this perspective, safety assessment should be one of the primary filters in ATM concept development. An early filtering of ATM design concepts on safety grounds can potentially avoid a costly development program that turns out to be ineffective, or an even more costly implementation program that fails. Although understanding this idea is principally not very difficult, it can be brought into practice only when an ATM safety assessment approach is available that provides appropriate feedback to the ATM designers at an early stage of the concept development (Fig. 1). Such an approach has been presented by Ref. [1] and this paper is based on this.

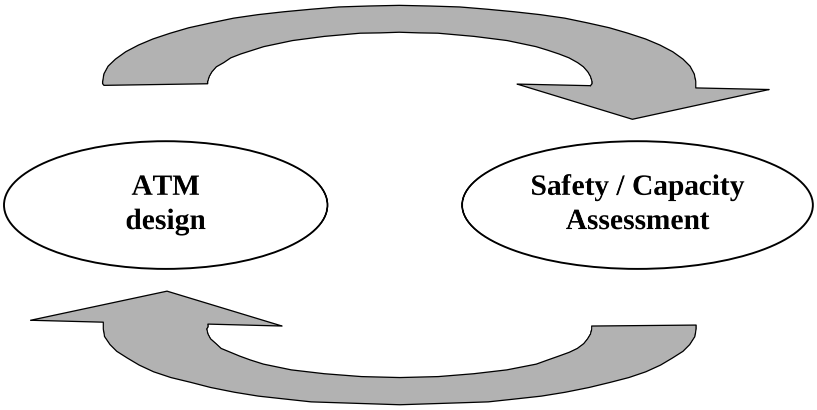


Figure 1: Safety feedback based ATM design.

This feedback should not only provide information on whether the design is safe enough, but it should also identify the safety-capacity bottlenecks. By now, consensus is building that appropriate ATM safety modeling approaches are needed to understand the mechanisms behind designing advanced ATM. It is also recognised that, once such an ATM safety modeling approach is available, a safety feedback based design approach of future ATM will become feasible [2], [3], [4].

Safety is a general notion that is typically studied from one of three different perspectives:

1. Safety perception (e.g., by pilot, controller, passenger, human society, etc.). An ATM design that is perceived as being unsafe will not easily be accepted by the humans involved. A positive perception about the safety of an ATM design is an implementation-critical requirement. By its very nature, however, safety perception is a subjective notion, and therefore insufficient to really approve safety-critical changes in ATM.
2. Dependability of a technical system (e.g., of a computer program, an aircraft navigation system, a satellite-based communication system, etc.). Dependability metrics are definitively objective. They are widely studied in literature (e.g., Refs. [5] and [6]). However, they have been developed to cover technical systems only (e.g., Refs. [7], [8] and [9]), and not the human operators and procedures of ATM (Ref. [10]).
3. Accident risk (e.g., for first, second and third parties in air transport). Accident risk metrics definitively are objective and are commonly in use for other human-controlled safety-critical operations such as in the chemical and nuclear industries (Ref. [11]). Two well-known International Civil Aviation Organisation (ICAO) adopted accident risk metrics are for collision of an aircraft with another aircraft during the en route phase, or with fixed obstacles during landing. A recent review of various accident risk metric possibilities in air transport is given in (Ref. [12]).

In view of the ATM safety assessment needs, the accident risk perspective has the best joint characteristics: 1) it implies the use of objective risk metrics; 2) it has proven its usability to human-controlled safety-critical operations; and 3) it is supported by ICAO. As such, in this paper ATM safety will be considered from an accident risk perspective, with emphasis on risk of collision between two aircraft.

For air traffic the fatal accident risks should be on the order of 10^{-7} - 10^{-10} per aircraft flight hour. To develop some feeling of the difficulty to assess such rare events, it is quite helpful to understand why the well-known fast-time simulators like National Airspace Systems Performance Analysis Capability (NASPAC), Reorganized ATC Mathematical Simulator (RAMS) or Total Airspace and Airport Modeller (TAAM) fall short for that purpose. One major shortcoming of these tools is that they are not really capable of modeling the aviation safety-critical combinations of non-nominal events; they often do not even model the single non-nominal events. Another major shortcoming is that an accident rate of, say,

10^{-9} per aircraft flight hour cannot in a practically reasonable way be reached through a straightforward simulation, because this would require a simulation of 10^{10} aircraft flight hours. This problem is well illustrated by the ATM safety iceberg (Fig. 2). To assess a catastrophic accident rate, one really needs to decompose the risk assessment problem into an effective hierarchy of simpler conditional assessment problems, in which simplicity means an appropriate combination of scope (e.g., volume of airspace) and depth (i.e., level of model detail) at each conditional assessment level. Indeed, tools like TAAM apply to assessments that address a broad scope in combination with a low level of non-nominal detail.

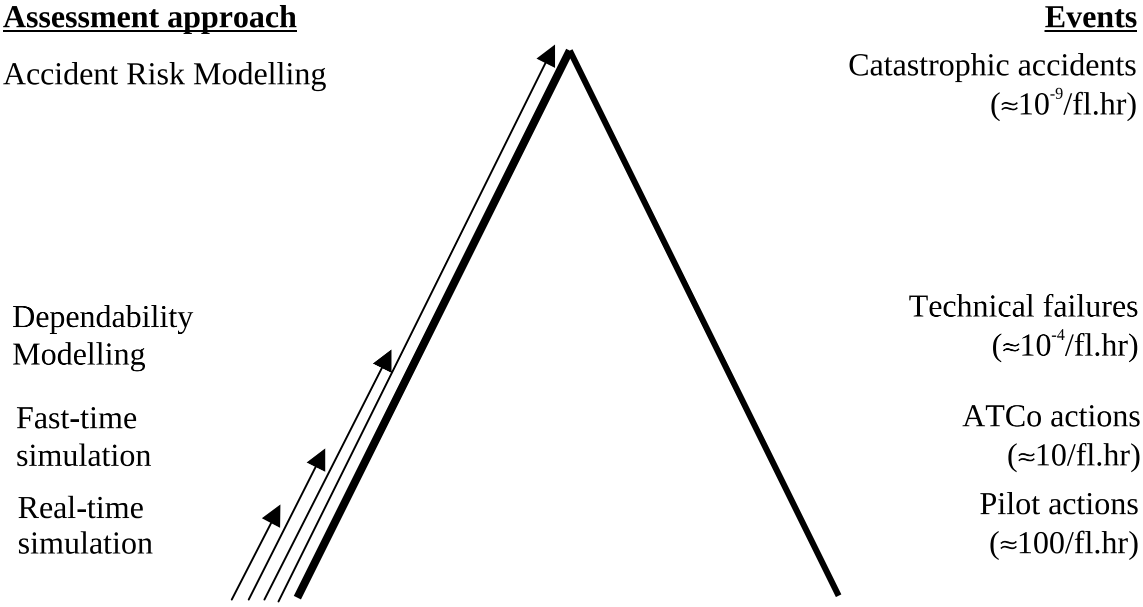


Figure 2: ATM safety iceberg.

In general, the accident risk assessment problem has been widely studied for other safety-critical operations, such as the nuclear and chemical industries, and for these applications, numerous techniques and tools have been developed. To take maximal advantage of this existing body of knowledge, we made a thorough study of the applicability of these techniques to accident risk assessment in air traffic [13]. A large variety of techniques has been identified, varying from qualitative hazard identification methods such as preliminary hazard analysis (PHA), common cause analysis (CCA), and failure mode and effect analysis (FMEA), through static assessment techniques such as fault tree analysis (FTA) and event tree analysis (ETA), to dynamic assessment techniques such as Petri net and Markov chain modeling, dynamic event trees, etc. [14]. Each of these techniques has advantages and disadvantages, but these appear to be minor in comparison to what is required for modeling ATM-related risk. The key finding is that the established techniques fail to support a systematic approach toward modeling stochastic dynamical behavior over time for complex interactions of highly distributed ATM (see Fig. 3). The established techniques would therefore force one to adopt a rather heuristic type of argumentation in trying to capture the complex interactions inherent to ATM.

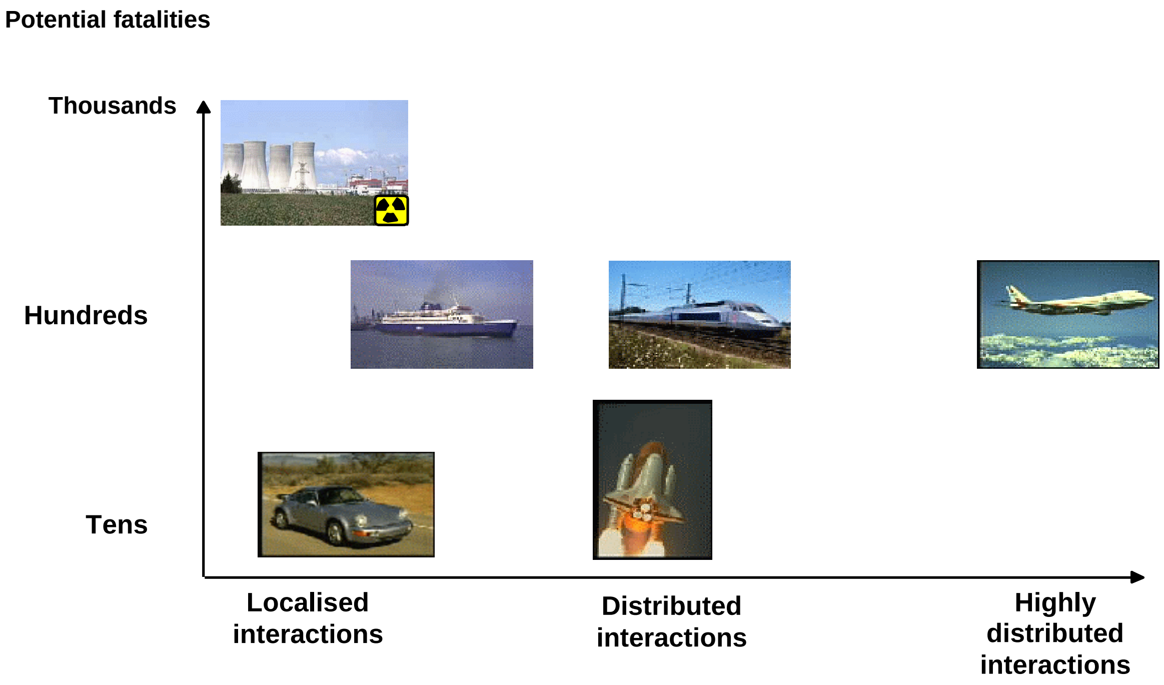


Figure 3: Potential fatalities and distribution level of ATM and other safety critical activities.

The basic ATM safety assessment needs have already been identified in Ref. [15]. This finding motivated the development of an adequate safety assessment approach within a project named Traffic Organization and Perturbation AnalyZer (TOPAZ). The scientific basis for this was the idea to explore a stochastic analysis framework [16], [17] that supports stochastic models in which both discrete and continuous variables evolve over continuous time, possibly affected by probabilistic disturbances, and the knowledge that this framework would be sufficiently general to properly model and evaluate ATM safety problems.

In the meantime, from parallel conducted studies on advanced ATM, it became clear that without an appropriate accident risk model it would be difficult to ever manage a cost-effective design of advanced ATM. In these studies three complementary perspectives have been considered: 1) the selection of route structures perspective [18], 2) a stochastic dynamical game perspective [19] and 3) an ATM overall validation perspective [20].

The accident risk assessment results obtained through stochastic analysis studies have initially been exploited toward the assessment of accident risk for staggered landings on converging runways at Schiphol [21], [22]. All this contributed to the development of both the novel accident risk assessment methodology and a growing suite of supporting tools. In this paper, emphasis is on the former, for the reason that an effective usage of the suite of tools requires firm background in the novel methodology.

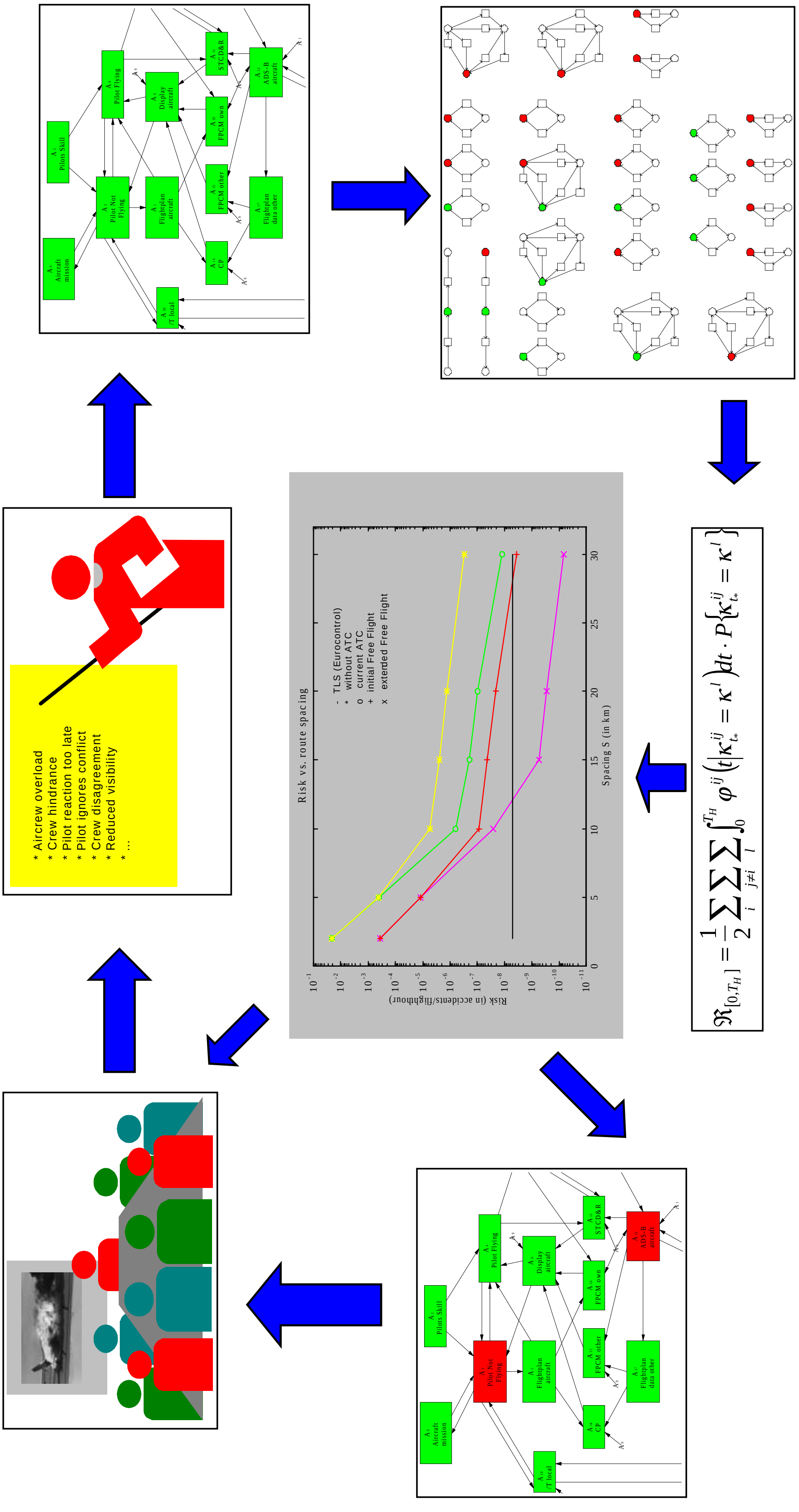
Recently, by a joint effort of EUROCONTROL and the Federal Aviation Administration (FAA), in collaboration with some key developers of aviation risk assessment tools, an overview has been produced that outlines the relevant approaches currently in development and/or in use for the safe separation assessment of advanced procedures in air traffic [23]. In addition to TOPAZ, four other collision risk directed approaches, Analytic Blunder Risk Model (ABRM), Airspace Simulation and Analysis for Terminal instrument procedures (ASAT), ICAO's Collision Risk Model (CRM) and Reduced Aircraft Separation Risk Assessment Model (RASRAM) [24], have been identified and reviewed. TOPAZ appeared to be most advanced in going beyond established approaches.

This paper is organised as follows. Section II gives an overview of the advanced methodology. Section III outlines the principles of the underlying stochastic dynamical framework. Section IV presents some example scenarios for the results of accident risk assessments. Section V gives concluding remarks on the methodology.

II. Accident Risk Assessment Methodology

The accident risk assessment methodology has been developed to provide designers of advanced ATM with safety feedback following a (re)design cycle. An illustrative overview of how such safety feedback is obtained during an assessment cycle is given in Fig. 4.

During such an assessment cycle, two types of assessments are sequentially conducted: first a qualitative safety assessment (illustrated by the upper drawings in Fig. 4), and then a quantitative safety assessment (illustrated by the middle and lower drawings in Fig. 4). The qualitative assessment starts with a systematic gathering of information about nominal and non-nominal behaviour of the concept design considered, concerning the human roles, the procedures, the technical systems, etc., and with involvement of all relevant experts. For the gathering of non-nominal information, explicit use is made of structured hazard identification sessions with a variety of experts and hazard databases. The resulting list of identified potential hazards is subsequently analyzed using established qualitative hazard analysis techniques to identify the safety-critical encounter scenarios and associated hazards, to select one or more of those safety-critical encounter scenarios for quantitative safety assessment, and to develop a modular system engineering type of representation of the ATM design (see upper right corner of Fig. 4). Such modular representation is easily recognizable and understandable for ATM designers, thus supporting an effective communication between ATM designers and safety analysts.



$$\Re_{[0,T_H]} = \frac{1}{2}\sum_i \sum_{j\neq i} \sum_l \int_0^{T_H} \varphi^{ij}\left(t \middle| \kappa_{t*}^{ij} = \kappa^l\right) dt \cdot P\left\{\kappa_{t*}^{ij} = \kappa^l\right\}$$

Figure 4: TOPAZ accident risk assessment cycle.

From this point on, the accident risk assessment cycle continues with the quantitative phase, which is based on stochastic modeling, stochastic analysis and numerical evaluation. First, an appropriate stochastic dynamical model instantiation is developed in an iterative way and with verification against the results of the qualitative safety assessment phase. Next, the accident risk is assessed for this stochastic dynamical model, and the safety criticalities are identified. Finally, these results are given back to the designers (see lower left corner of Fig. 4).

To from a natural balance between the creative mode of the designers and the critical mode of the safety analysts, we have identified a definitive need for the safety analysts to use a conservative approach when adopting assumptions during the risk analysis. Obviously, the design team need not always agree with these conservative assumptions and should be aware that a negative outcome of a conservative assessment cycle does not mean that the design is unsafe; it just means that sufficient safety has not been proven during that cycle. This natural balance between designers and safety analysts means that both parties should be open to accept each other's views as being of mutual use. Conservatism could be reduced by refining the instantiated stochastic dynamical model on the appropriate issues identified by the designers. For the designers it could even be more effective to relax potential safety criticalities through redesign, rather than awaiting a potential accident risk modeling based improvement.

Underlying an accident risk assessment cycle is a stochastic analysis framework, which allows distinguishing the following five activities:

1. develop a stochastic dynamical model for the situation considered;
2. where necessary develop appropriate cognitive models for human operators involved;
3. perform the stochastic analysis necessary to decompose the risk assessment;
4. execute the various assessment activities (e.g., through Monte Carlo simulation, numerical evaluation, mathematical analysis, or a combination of these); and
5. validate the risk assessment exercise.

More details on these five activities are given in the following sections.

A. Develop a Stochastic Dynamical Model

The aim of this development is to represent for the selected encounter scenarios the results from the qualitative safety assessment in the form of a stochastic differential equation (SDE) on a hybrid state space. The reason for aiming for such SDE representation is twofold: 1) it provides a very widely applicable class of causal models for stochastic dynamical situations such as in ATM; and 2) it allows the exploration of powerful mathematical tools from the theory of stochastic analysis (e.g., Refs. [25], [26], [16]). Unfortunately, the direct identification of the SDE model would be very complicated for most ATM situations. In addition to a very large state space of the corresponding SDE, there are many interactions between the many state components. This requires a systematic approach to develop an SDE instantiation for such complex situations. Such approach has been introduced through the development of a specific type of Petri Net [27], [28], which we refer to as the dynamically colored Petri net (DCPN). Through a DCPN instantiation, an SDE instantiation can be done systematically while the result is transparent. Once a DCPN instantiation has been completed, the result defines an SDE on a hybrid state space. Obviously, a logical part of the DCPN instantiation is to verify the resulting DCPN against the information that is gathered during the qualitative safety assessment phase.

B. Cognitive Human Modeling

When assessing ATM safety, a key role is played by procedures, human operators, and their responsibilities. At present, the view on human reliability has shifted from a context-free error centered approach in which unreliability is modeled through failures of human information processing, toward a contextual perspective in which human actions are the product of human internal states, strategies, and the environment. By now, it is a widely accepted belief [29], [30], [31] that for modeling of the human the established human reliability analysis (HRA) techniques fall short for complex situations, and that one should rather aim for contextual performance models that are based on generally applicable human cognition and responsibility principles. It should also be noticed that in the HRA widely used skill-, rule-, and knowledge-based errors [32] essentially fall short in paying proper attention to situations that fall beyond procedures. For example, situations in which the operator chooses to let an even more urgent problem receive attention when the subjectively available time is short or when high workload causes one to make quick decisions, without bothering excessively about the quality of those decisions. It should be noticed that these effects are inextricably bound with human flexibility and the ability of humans to deal with unforeseen situations. When assessing ATM safety, it is necessary to take these aspects of human performance into account.

The main benefits expected from contextual models is that they provide better feedback to designers and that they remove the need to use overly conservative individual submodels for relevant operator actions that may blur understanding of how safety is achieved in ATM. To develop appropriate models for this, mathematicians and psychologists are jointly developing high-level models of cognitive human performance, through a sequence of studies (e.g., Refs. [33] and [34]). At this moment this collaboration has led to a novel contextual human task-network model, which is formulated in terms of a DCPN and which effectively combines the cognitive modes of Hollnagel [30] with the multiple resources theory of Wickens [35], the classical slips/lapses model [32], and the human capability to recover from errors [29]. In addition, we have developed a model for the evolution of situational awareness errors. Compared with those considered in a recent study [36], our approach appears to be an innovative one.

C. Perform Stochastic Analysis

Although it definitively is possible to realize a straightforward Monte Carlo simulation of the SDE model, it is clear from the earlier discussion that this will not be really effective for the assessment of catastrophic risks in aviation. To develop an effective approach to the numerical evaluation of an SDE model, the SDE should be analyzed first by mathematicians with the appropriate background in the theory of stochastic analysis. At this moment, this is done on a case-by-case basis. For each case, the aim is to analyze the SDE model such that its numerical evaluation can be done by decomposition into a logical sequence of fast-time simulations, Monte Carlo simulations, and/or analytical evaluations. The aim always is to first decompose the risk assessment problem into several conditional assessment problems for which appropriate assessment techniques are available or feasible. The main principle we are using for identifying an appropriate decomposition is the following: under quite general conditions, the solution of an SDE is a strong Markov process. This means that the Markov property also holds true for stopping times (sometimes called Markov times). These stopping times serve as the mathematical powertool to decompose the risk assessment for an SDE model. So far, this approach appears to work satisfactorily for all situations evaluated.

D. Execute the Various Assessment Activities

Typically, the resulting sequence of conditional assessments is as follows:

1. Run a conventional fast time simulation (e.g., with TAAM) to identify traffic densities and encounter type frequencies.
2. Input these traffic densities and encounter type frequencies to a safety-directed human simulator to identify appropriate pilot and/or controller characteristics.
3. Input these conditional human characteristics to a Monte Carlo simulation that identifies and statistically analyzes critical conditional events, such as incidents.
4. Input these critical conditional event characteristics to a Monte Carlo simulation that identifies potential accident characteristics.
5. Input these potential accident characteristics to a conditional collision risk analyzer.
6. Transform all results from the preceding conditional assessments into appropriate safety metrics.
7. Identify the safety-separation and/or safety-modeling bottlenecks of the specifically modeled ATM concept/scenario.

For each of these activities, except activity 1, dedicated computer tools have been and are being further developed within the TOPAZ project. The splitting of activities 3, 4 and 5 from each other usually appears to be the most challenging one, for the very reason that often there are many dependencies between various elements of a hazardous air traffic situation. To handle this in a valid way, we make use of a mathematical framework, the basis of which is explained in Section III.

E. Validation of the Risk Assessment Exercise

A crucial issue concerns the validation that a risk assessment exercise is performed to an acceptable degree, without the need to first employ very expensive large-scale real-time simulations of new concepts. Because of our underlying stochastic analysis framework, such a validation can be done through executing the following activities:

1. Judge the level of conservatism of the assumptions adopted for the development of the DCPN instantiation for the situation considered. This should be done through active involvement of operational and design experts.
2. Verify the correctness of the instantiated DCPN vs the results of the qualitative assessment and the assumptions adopted. This should be done by stochastic analysis experts, with at least one who has not been involved with the DCPN instantiation.
3. Verify the correctness of the mathematical transformations applied to the instantiated stochastic dynamical model. This should be done by applying mathematical tools from stochastic analysis theory.
4. Verify that the various assessment activities have been executed according to the unambiguous mathematical model developed, including the decomposition. This should be done by stochastic analysis experts.

III. Mathematical Framework

Each DCPN instantiation can be represented by an SDE on a hybrid state space [28], which has a strong Markov process $\{\xi_t\}$ on a hybrid state space as its unique solution. The hybrid state process $\{\xi_t\}$ has two components, i.e., $\xi_t = (x_t, \theta_t)$, with x_t the component assuming values in a Euclidean space and with θ_t the component assuming values in a discrete space. From the theory of Markov processes it then follows that it is possible to characterise the evolution of the density distribution $p_{\xi_t}(\xi)$ of the joint process through a well-defined differential equation in function space:

$$\frac{\mathrm{d}}{\mathrm{d}t} p_{\xi_t}(\xi) = \mathcal{A} p_{\xi_t}(\xi)$$

with $\mathcal{A}$ an operator defined by the Markov process $\{\xi_t\}$. Because of the strong Markov property, this differential equation also applies under the condition of an $\{\xi_t\}$-adapted stopping time τ (also referred to as Markov time):

$$\frac{\mathrm{d}}{\mathrm{d}t} p_{\xi_{t|\tau}}(\xi) = \mathcal{A} p_{\xi_{t|\tau}}(\xi), \quad \text{for} \quad t > \tau .$$

It is particularly relevant to notice that these equations are well known for Markov chains, i.e., Markov processes with discrete state space, which have shown to be very useful in the development of advanced dependability and performability assessment methodology (e.g., Refs. [37] and [38]). For hybrid state Markov processes, this equation is well known in Bayesian estimation theory (e.g., Ref. [16]) and this for example has led to advanced multitarget multisensor tracking applications (e.g., Ref. [39]).

The preceding equations imply that once the scenario to be assessed on collision risk has been represented through a DCPN instantiation, all probabilistic properties are well defined, including the collision risk. Let y_t^i and v_t^i be the components of x_t that represent the three-dimensional location and the three-dimensional velocity of aircraft i, $i \in \{1,...,n\}$. Let $y_t^{ij} = y_t^i - y_t^j$, let $v_t^{ij} = v_t^i - v_t^j$, and let D^{ij} be the area such that $y_t^{ij} \in D^{ij}$ means that at moment t the physical volumes of aircraft i and j are not separated anymore (i.e., they have collided). Each time the process y_t^{ij} enters the area D^{ij}, we note that an incrossing occurs, and each time the process y_t^{ij} leaves the area D^{ij}, we note that an outcrossing occurs. The first incrossing for the pair (i,j) is a collision for that pair. If we assume that the relative speed v_t^{ij} is very rapidly going to zero as long as y_t^{ij} resides in D^{ij}, the chances are zero that there is more than one incrossing per aircraft pair, and thus the expected number of incrossings equals the expected number of collisions. Following [40], the expected number $\Re_{[0,T]}$ of incrossings, or collisions, between aircraft pairs in the time-interval $[0,T]$ satisfies:

$$\Re_{[0,\mathrm{T}]} = \sum_{i=1}^{n} \sum_{j>i}^{n} \int_{0}^{T} \varphi^{ij}(t)\,\mathrm{d}\,t$$

with $\varphi^{ij}(t)$ the incrossing rate, which is defined by:

$$\varphi^{ij}(t) = \lim_{\Delta \downarrow 0} \Pr\left\{ y_t^{ij} \notin D^{ij}, y_{t+\Delta}^{ij} \in D^{ij} \right\} / \Delta$$

In Ref. [40] it is also shown that $\varphi^{ij}(t)$ is well defined and can be evaluated under non-restrictive assumptions as a function of the probability density of the joint relative state (y_t^{ij},v_t^{ij}). In general, a characterization of this probability density is complex, especially since there are combinatorially many types of non-nominal events. A plausible way out of this is by conditioning on classes of non-nominal events, where those non-nominal events are placed in the same class if they have a similar impact on the subsequent evolution of the relative state process $\{y_t^{ij},v_t^{ij}\}$. This is done through 1) defining an appropriate event sequence classification process $\{\kappa_t\}$, such that the joint process $\{\xi_t,\kappa_t\}$ is a strong Markov process as well, and 2) subsequently identifying an appropriate $\{\xi_t,\kappa_t\}$-adapted stopping time τ^{ij} such that there is a zero probability that the pair (i,j) collides before τ^{ij}. With this, the preceding equations can be transformed into:

$$\mathfrak{R}_{[0,T]} = \sum_{i=1}^{n} \sum_{j>i}^{n} \sum_{\kappa} \int_{\tau^{ij}}^{T} \varphi^{ij}\left(t \,\middle|\, \kappa_{\tau^{ij}} = \kappa\right) \mathrm{d}\, t \cdot \Pr\left\{\kappa_{\tau^{ij}} = \kappa\right\}$$

with $\varphi^{ij}\left(t \,\middle|\, \kappa_{\tau^{ij}} = \kappa\right)$ the conditional incrossing rate, being defined for $t \geq \tau^{ij}$ by:

$$\varphi^{ij}\left(t \,\middle|\, \kappa_{\tau^{ij}} = \kappa\right) = \lim_{\Delta \downarrow 0} \Pr\left\{y_t^{ij} \notin D^{ij}, y_{t+\Delta}^{ij} \in D^{ij} \,\middle|\, \kappa_{\tau^{ij}} = \kappa\right\} \Big/ \Delta$$

In Fig. 5, the equation for $\mathfrak{R}_{[0,T]}$ is presented in the form of a tree, in which $f^{ij}(\kappa)$ is short for

$$\int_{\tau^{ij}}^{T} \varphi^{ij}\left(t \,\middle|\, \kappa_{\tau^{ij}} = \kappa\right) \mathrm{d}\, t \cdot \Pr\left\{\kappa_{\tau^{ij}} = \kappa\right\}$$

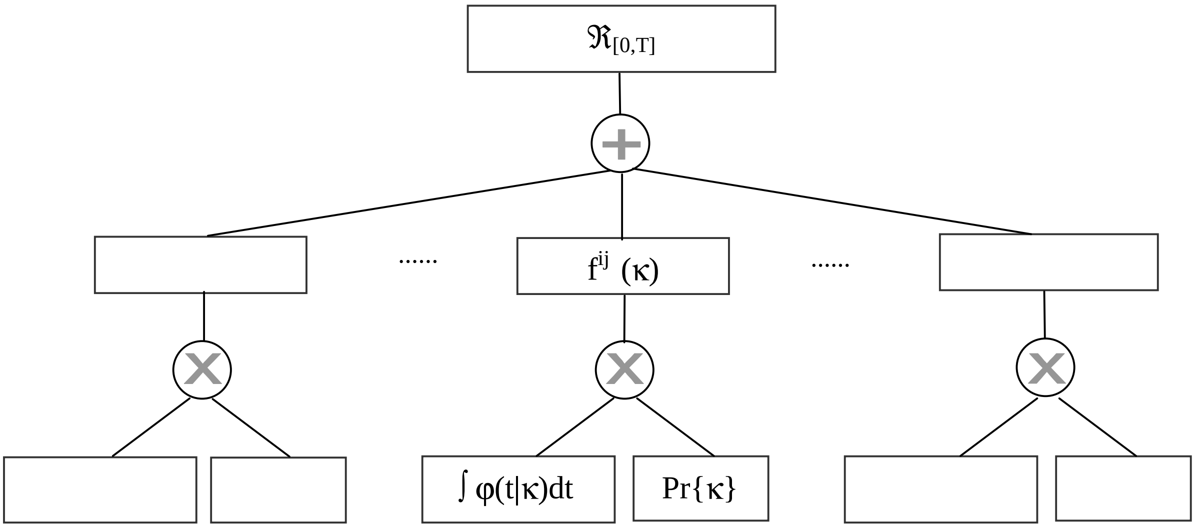


Figure 5: Collision risk tree.

This tree has some resemblance with the well-known fault tree. However, because of the underlying stochastic and physical relations, our new tree differs significantly and is called a collision risk tree.

For the quantification of the boxes in the collision risk tree, use is made of three types of evaluations:

1. Monte Carlo simulations of the DCPN to quantify $\Pr\left\{\kappa_{\tau^{ij}} = \kappa\right\}$ and the statistical properties of the relevant DCPN components at the stopping time τ^{ij}.

2. Evaluations of the evolution of the relative aircraft states from stopping time τ^{ij} on, and for each $\kappa_{\tau^{ij}} = \kappa$. If complexity requires, this process can even be done for a sequence of increasing stopping times.
3. Numerical evaluation of

$$\int_{\tau^{ij}}^{T} \varphi^{ij}\left(t \middle| \kappa_{\tau^{ij}} = \kappa\right) \mathrm{d}\, t$$

using the generalized Reich equation of Ref. [40]; see also Ref. [41].

IV. RNP1 in Conventional and Airborne Separation Assurance Scenario Examples

In this section, the accident risk assessment approach is used to evaluate a simple scenario of two en route traffic streams, flying in opposite directions, all at one single flight level. This rather hypothetical scenario has been developed by EUROCONTROL with the aim to learn how ATC influences accident risk, and how far the nominal separation *S* between opposite RNP1 traffic streams can safely be reduced. The specific details of this scenario are [42]:

1. Straight route, with two traffic lanes (Fig. 6),
2. Flight plans contain no lane changes,
3. Parameter *S* denotes distance between the two lanes,
4. Opposite traffic flows along each lane,
5. Aircraft fly at one flight level only,
6. Traffic flow per lane is 3.6 aircraft/hour,
7. All aircraft nominally perform RNP1 with 95% of the time within 1 n mile,
8. None of the aircraft are equipped with Traffic Alert and Collision Avoidance System (TCAS),
9. Target level of safety is 5×10^{-9} accidents/flight hour, [43].

This simple scenario is considered for the following four ATM concepts:

A. Procedural separation only. In this case, there is no air traffic control (ATC) surveillance system. This is the type of situation encountered with traffic over the North Atlantic.

B. ATC based only on ahort-term conflict alert (STCA). In this case there is radio/telephony (R/T) communication, but it is assumed that ATC is doing nothing unless its STCA system issues an alert, thus assuming no monitoring by the air traffic controller (ATCo). It should be noted that this differs significantly from conventional ATC, in which an executive controller autonomously monitors and issues corrective actions, while STCA is a safety net only.

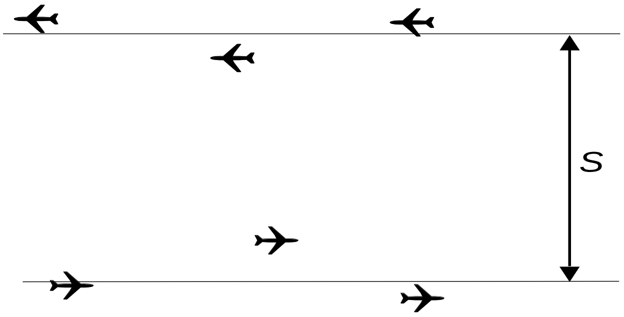


Figure 6: Opposite direction traffic in a dual lane route.

C. Basic airborne separation assurance. In this case, there is automatic dependent surveillance broadcast (ADS-B) surveillance and R/T between aircraft, but there is no ATC. For this concept it is assumed that aircraft behave cooperatively, in the sense that when an aircraft's conflict detection and resolution (CDR) system detects a conflict with another aircraft, then its pilot will try to make an avoidance maneuver. Thus, in most cases both pilots will try to make an avoidance maneuver.

D. Negotiated airborne separation assurance, a design that is explicitly due to the feedback received from accident risk assessments conducted for concepts A, B and C. For this concept, it is assumed that aircraft also behave cooperatively during conflict-free trajectory planning. Thus, in addition to ADS-B surveillance and R/T, there also is a data link between aircraft to exchange and negotiate conflict-free trajectory plans that are assumed to extend 5 min or more into the future.

Obviously, for each of these four ATM concepts there are various traffic navigation and encounter scenarios that deserve an accident risk evaluation. We believe, however, that it is most effective to understand the safe separation issues for a simple traffic navigation and encounter scenario first, before considering other and more complicated scenarios.

For each of the four ATM concepts, the accident risk assessment methodology and aupporting tool set have been used to conservatively assess accident risk for the preceding scenario, as a function of the spacing parameter *S*. The resulting accident risk curves are presented in Fig 7. Because all four curves are based on conservative modeling assumptions for the ATM situations considered, they provide an upper bound for the true accident risk.

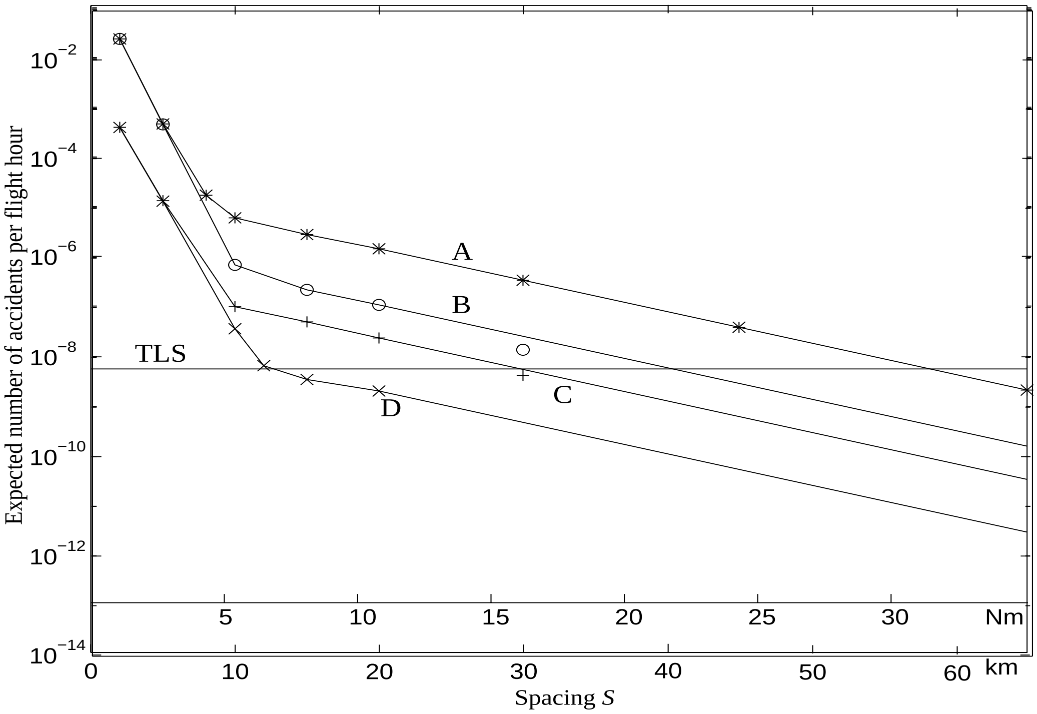


Figure 7: Accident risk for the opposite traffic scenario, as a function of spacing parameter S, for the four ATM concepts considered: A) procedural separation, B) STCA-based ATC, C) basic airborne separation assurance, D) negotiated airborne separation assurance. The accident risk unit used is from ICAO, where one collision between two aircraft counts for two "accidents".

These results are obtained over a period of two years during three subsequent studies. The first en route study [42] was conducted for EUROCONTROL and covered ATM concepts A and B. The assessment of concept A was rather straightforward and could also have been done with ICAO's CRM. For the assessment of the other three concepts, however, full use has been made of the accident risk assessment methodology. Concept B has been assessed during an initial study for Eurocontrol [42]. Concept C has been developed [44] and assessed [45] during studies within NASA's Free Flight research program. The safety assessment results from concepts A, B and C have subsequently been fed back [46] to enable the development of the design concept D, and subsequently to assess it on accident risk [47].

The risk curves in Fig. 7 show that for RNP1 performing aircraft, the ATM concept may have quite an impact on the selection of the spacing parameter *S* within a straight dual lane route structure. For the four ATM concepts considered, it has been shown that the spacing S can safely be reduced to 31, 22, 16, and 7 n miles for ATM concepts A, B, C and D, respectively. The large value of 31 n miles for concept A is not a real surprise, such large values are well known for procedural traffic situations over the ocean. The results for concept B show that STCA really is a safety that provides at least a factor 15 in safety when compared with concept A for sufficiently large *S*. Apparently, this STCA safety net alone falls short to support the kind of spacings necessary for busy fixed route traffic situations. This finding confirms the prior expectation that concept B is not representative for conventional ATC.

Rather unexpectedly, the cooperative basic airborne separation concept C appears to perform better than concept B. The reason appeared to be that with the ground-based concept B there is one single monitoring and decision-making loop (surveillance-STCA-ATCo-R/T-pilot-aircraft), whereas for the cooperative airborne-based concept C each of the two encountering aircraft has a monitoring and decision-making loop (surveillance-CDR-pilot-aircraft) which are partly independent. As a result, the safety net of concept C leads to a factor 5 lower risk than concept B for the same spacing, or allows to safely reduce *S* from 22 n miles to 16 n miles. Obviously, such improved safety net still falls short to support the kind of spacings necessary for busy fixed route traffic situations. Thus in view of their safe spacing values of 22 n miles and 16 n miles, concepts B and C do not support spacings that are required for busy fixed route situations over the continent.

Finally, the cooperative negotiated airborne separation assurance concept D allows such low spacing values. This is not a coincidence, but it is the result of effectively making use of accident risk assessment feedback from A, B and C. It appeared that for all three of these concepts, the safe spacing was determined by the effects of the exponential tails of large deviations due to non-nominal situations. Thus, the design objective for concept D was to reduce those non-nominal effects to a level below the target level of safety (TLS). To accomplish this, the two monitoring and decision-making loops of concept C have been extended with a largely independent and cooperative conflict-free-planning loop. The curve for concept D shows that this worked out successfully, by which the safe spacing value for concept D is governed by the RNP1-Gaussian navigation error characteristics, rather than by the exponential tails due to non-nominal situations.

V. Concluding Remarks

This paper has given an outline of an accident risk assessment methodology to assess advanced ATM on midair collision risk and has illustrated that this approach may provide effective feedback to designers of advanced ATM. From this outline it has become clear that this methodology exhibits several remarkable features, such as:

1. It applies established techniques during a qualitative assessment phase only.
2. Quantification is based on stochastic dynamical modeling.
3. It uses powerful tools from the theory of stochastic analysis.

4. It handles complex interactions between different ATM elements.
5. It incorporates advanced human cognitive modeling.
6. It incorporates the generalized Reich collision risk model.
7. It provides effective feedback to ATM concept designers.
8. Validation of a risk assessment exercise forms part of the methodology.

It has also become clear that currently a high level of expertise in stochastic analysis is required for an effective application of the methodology. One should, however, be aware that the need for sophisticated mathematical expertise is well accepted in other complex design areas of civil aviation, such as the area of aerodynamic optimization of aircraft structures.

Obviously, within an overall ATM concept, a large variety of relevant aircraft encounter scenarios can be identified. As such, it is important to notice that our DCPN instantiation for a particular ATM concept mainly depends on the ATM concept and only marginally on the encounter scenario. Thus, the DCPN instantiations for the four RNP1 based ATM concepts in Section IV can be extended relatively simply to other encounter scenarios. This also means that it should be possible to identify classes of encounter scenarios so that it is sufficient to perform an accident risk assessment for one scenario from each class only.

In this paper, the methodology of accident risk assessment has been concentrated on the risk of midair collision. Because of the generality of the methodology, however, it is also applicable to other accident risks in air traffic, such as risk induced by runway incursion, controlled flight into terrain, etc. We have, for example, already made good progress in the extension of the accident risk assessment methodology with a probabilistic model for wake vortex induced accident risk [48].

References

[1] Blom, H.A.P., Bakker, G.J., Blanker, P.J.G., Daams, J., Everdij, M.H.C., and Klompstra, M.B., "Accident Risk Assessment for Advanced ATM," *2nd USA/Europe Air Traffic Management R&D Seminar*, FAA/EUROCONTROL, 1998, also NLR Rept. TP-99-015, Amsterdam, 1999.

[2] Haraldsdottir, A., Alcabin, M.S., Burgemeister, A.H., Lindsey, C.G., Makins, N.J., Schwab, R.W., Shakarian, A., Shontz, W.D., Singleton, M.K., van Tulder, P.A., and Warren, A.W., "Air Traffic Management Concept Baseline Definition," NEXTOR Rept. RR-97-3, Boeing, Seattle, WA, 1997.

[3] Odoni, A.R., Bowman, J., Delahaye, D., Deyst, J.J., Feron, E., Hansman, R.J., Khan, K., Kuchar, J.K., Pujet, N., and Simpson, R.W., "Existing and Required Modeling Capabilities for Evaluating ATM Systems and Concepts," sponsored by NASA under Grant no. NAGZ-997, Massachusetts Inst. of Technology, Cambridge, MA, March 1997.

[4] EVAS, "EATMS Validation Strategy Document," Ed. 1.1, Eurocontrol, Brussels, June 1998.

[5] Randell, B. (ed.), *Predictably Dependable Computing Systems*, Springer-Verlag, Berlin, 1995.

[6] "DAAS Dependability Approach to ATM Systems" Final Report, European Commission, Brussels, 1995.

[7] "ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," S-18 Committee, Society of Automotive Engineers, Inc., March 1994.

[8] "ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems," Systems Integration Requirements Task Group AS-1C, Avionics Systems Division, Society of Automotive Engineers, Inc., Sept. 1995.

[9] "Air Navigation System Safety Methodology," Ed. 0.4, Working Draft, EATCHIP, Eurocontrol, Brussels, 1996.

[10] Klompstra, M.B., and Everdij, M.H.C., "Evaluation of JAR and EATCHIP Safety Assessment Methodologies," National Aerospace Laboratory NLR, NLR Rept. CR 97678 L, Amsterdam, 1997.

[11] "Risk assessment, Report of a Royal Society Study Group", Royal Society, London, 1983.

[12] Moek, G., Blom, H.A.P., Klompstra, M.B., Beaujard, J.P., Kelly, C., Mann, J., Clarke, L., and Marsh, D., "Methods and Techniques," National Aerospace Laboratory NLR, GENOVA WP3, NLR Rept. TR-98595-PT-1, Amsterdam, 1997.

[13] Everdij, M.H.C., Klompstra, M.B., Blom, H.A.P., and Fota, O.N., "Evaluation of Hazard Analysis Techniques for Application to En Route ATM," National Aerospace Laboratory NLR, MUFTIS Final Rept. on Safety Model, Part I, National Aerospace Laboratory NLR, NLR Rept. TR 96196 L, Amsterdam, 1996.

[14] Aldemir, T., Siu, N.O., Mosleh, A., Cacciabue, P.C., and Göktepe, B.G. (eds.), *Reliability and Safety Assessment of Dynamic Process Systems*, Springer-Verlag, Berlin, 1994.

[15] Blom, H.A.P., "The Layered Safety Concept, an Integrated Approach to the Design and Validation of Air Traffic Management Enhancements," National Aerospace Laboratory NLR, NLR Rept. TP 92046 L, Amsterdam, 1992.

[16] Blom, H.A.P., "Bayesian Estimation for Decision-Directed Stochastic Control," Ph.D. Dissertation, Delft University of Technology, Delft, The Netherlands, 1990.

[17] Everdij, M.H.C., Klompstra, M.B., and Blom, H.A.P., "Development of Mathematical Techniques for ATM Safety Analysis, MUFTIS Final Report on Safety model, Part II," National Aerospace Laboratory NLR, NLR Rept. TR 96197 L, Amsterdam, 1996.

[18] Blom, H.A.P., and Bakker, G.J., "A Macroscopic Assessment of the Target Safety Gain for Different En Route Airspace Structures Within SUATMS," National Aerospace Laboratory NLR, NLR Rept. CR 93364 L, Amsterdam, 1993.

[19] Blom, H.A.P., Klompstra, M.B., and Bakker, G.J., "Air Traffic Management as a Multi-Agent Stochastic Dynamic Game Under Partial State Observation," *Proceedings of the 7th*

IFAC/IFORS Symposium on Transportation Systems, International Federation of Automatic Control, 1994, pp. 249-254, also National Aerospace Laboratory NLR, Rept. TP 94363U, Amsterdam, 1994.

[20] Blom, H.A.P., Hendriks, C.F.W., and Nijhuis, H.B., "Assess Necessary Validation Developments," National Aerospace Laboratory NLR, VAPORETO WP3 Final Rept.: NLR Rept. CR 95524 L, Amsterdam, 1995.

[21] Bakker, G.J., Blom, H.A.P., and Everdij, M.H.C., "Collision Risk Evaluation of the Dependent Converging Instrument Approach (DCIA) Procedure Under Gaussian Deviations from Expected Missed Approach Paths," National Aerospace Laboratory NLR, NLR Rept. CR 95322 L, Amsterdam, 1995.

[22] Everdij, M.H.C., Bakker, G.J., and Blom, H.A.P., "Application of Collision Risk Tree Analysis to DCIA/CRDA Through Support of TOPAZ," National Aerospace Laboratory NLR, NLR Rept. CR 96784 L, Amsterdam, 1996.

[23] Cohen, S. and Hockaday, S. (eds.), "A Concept Paper for Separation Safety Modeling, an FAA/EUROCONTROL Cooperative Effort on Air Traffic Modeling for Separation Standards," FAA and EUROCONTROL, Brussels, May 1998.

[24] Sheperd, R., Cassell, R., Thava, R., and Lee, D., "A Reduced Aircraft Separation Risk Assessment Model," *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, AIAA, Reston, VA, August 1997.

[25] Elliott, R.J., *Stochastic Calculus and Applications*, Springer-Verlag, New York, 1982.

[26] Davis, M.H.A., "Piecewise Deterministic Markov Processes: A General Class of Non-Diffusion Stochastic Models," *Journal Royal Statistic Society (B)*, Vol. 46, 1984, pp. 353-388.

[27] Everdij, M.H.C., Blom, H.A.P., and Klompstra, M.B., "Dynamically Coloured Petri Nets for Air Traffic Management Safety Purposes," *Preprints 8th IFAC Symposium on Transportation Systems*, edited by M. Papageorgiou, A. Pouliezos, Intelligent Technological Systems Lab., Technical University of Crete, 1997, pp. 184-189, also National Aerospace Laboratory NLR, NLR Rept. TP-97-493, Amsterdam, 1997.

[28] Everdij, M.H.C., and Blom, H.A.P., "Piecewise Deterministic Markov Processes Represented by Dynamically Coloured Petri Nets," National Aerospace Laboratory NLR, NLR Rept. TP-2000-428, Amsterdam, 2000.

[29] Amalberti, R., and Wioland, L., "Human Error in Aviation," *International Aviation safety Conference*, edited by H. Soekkha, VSP, Utrecht, The Netherlands, 1997, pp. 91-108.

[30] Hollnagel, E., *Human Reliability Analysis, Context and Control*, Academic Press, London, 1993.

[31] Bainbridge, L., "The Change of Concepts Needed to Account for Human Behaviour in Complex Dynamic Tasks," *1993 International Conference on Systems, Man and Cybernetics*, 1993, pp. 126-131.

[32] Reason, J., *Human Error*, Cambridge University Press, Cambridge, MA, 1990.

[33] Biemans, M.C.M., and Daams, J., "Human Operator Modeling to Evaluate Reliability, Organisation and Safety," National Aerospace Laboratory NLR, NLR Rept. TR 98073, Amsterdam, 1997.

[34] Daams, J., and Nijhuis, H.B., and Blom, H.A.P., "Human Operators Controllability of ATM Safety, ARIBA," National Aerospace Laboratory NLR, NLR Rept. TR-99575, Amsterdam, 1999.

[35] Wickens, C.D., *Engineering, Psychology and Human Performance*, Merrill, Columbus, OH, 1992.

[36] "A Designers Guide to Human Performance Modeling," Advisory Group for Aerospace Research and Development, AGARD, Advisory Rept. 356, Neuilly-Sur-Seine, France, Dec. 1998.

[37] Pattipati, K.R., Li, Y., and Blom, H.A.P., "A Unified Framework for the Performability Evaluation of Fault-Tolerant Computer Systems," *IEEE Transactions on Computers*, Vol. 42, No. 3, 1993, pp. 312-326.

[38] Fota, O.N., Kaaniche, M., and Kanoun, K., "A Modular and Incremental Approach for Building Complex Stochastic Petri Net Models," *First International Conference on Mathematical Methods in Reliability*, 1997, pp. 151-158.

[39] Blom, H.A.P., Hogendoorn, R.A., and Van Doorn, B.A., "Design of a Multisensor Tracking System for Advanced Air Traffic Control," *Multitarget-Multisensor Tracking*, edited by Y. Bar-Shalom, Vol. II, Artech House, Norwood, MA, 1992, pp. 31-63, also National Aerospace Laboratory NLR, Rept. TP 910164, Amsterdam, 1991.

[40] Bakker, G.J., and Blom, H.A.P., "Air Traffic Collision Risk Modeling," *Proceedings of the 32nd IEEE Conference on Decision and Control*, Vol. 2, Institute of Electrical and Electronics Engineers, New York, 1993, pp. 1464-1469, also National Aerospace Laboratory NLR, Rept. TP 93292, Amsterdam, 1993.

[41] Bakker, G.J., Kremer, H.J., and Blom, H.A.P., "Geometric and Probabilistic Approach Towards Conflict Prediction," *3rd USA/Europe Air Traffic Management R&D Seminar*, FAA/ EUROCONTROL, 2000, also National Aerospace Laboratory NLR, Rept. TP-2001-627, Amsterdam, 2001.

[42] Everdij, M.H.C., Bakker, G.J., Blom, H.A.P., and Blanker, P.J.G., "Demonstration Report in Preparation to Designing EATMS Inherently Safe," National Aerospace Laboratory NLR, TOSCA II WP4 Phase I Rept., NLR, Amsterdam, 1997, also National Aerospace Laboratory NLR, Rept. CR 97419L, Amsterdam, 1997.

[43] "ICAO Annex 11 – Air Traffic Services," 12th ed., incorporating amendments 1-38, green pages, attachment B, paragraph 3.2.1., International Civil Aviation Organisation, Montreal, July 1998.

[44] Hoekstra, J.M., Ruigrok, R.C.J., and Van Gent, R.N.H.W., "Conceptual Design of Free Flight Cruise with Airborne Separation Assurance," National Aerospace Laboratory NLR, NLR Rept. TP 98252, Amsterdam, 1997.

[45] Daams, J., Bakker, G.J., and Blom, H.A.P., "Safety Evaluation of an Initial Free Flight Scenario with TOPAZ," National Aerospace Laboratory NLR, NLR Rept. TR 98098, Amsterdam, 1998.

[46] Van Gent, R.N.H.W., Hoekstra, J.M., and Ruigrok, R.C.J., "Free Flight with Airborne Separation Assurance," *Proceedings CEAS symposium*, 1997; also National Aerospace Laboratory NLR, NLR Rept. TP-98286, Amsterdam, 1998.

[47] Daams, J., Bakker, G.J., and Blom, H.A.P., "Safety Evaluation of Encounters Between Free-Flight Equipped Aircraft in a Dual Route Structure," National Aerospace Laboratory NLR, NLR Rept. TR-99577, Amsterdam, 1998.

[48] Kos, J., Blom, H.A.P., Speijker, L.J.P., Klompstra, M.B., and Bakker, G.J., "Probabilistic Wake Vortex Induced Accident Risk Assessment," *3rd USA/Europe Air Traffic Management R&D Seminar*, FAA/EUROCONTROL, 2000, also National Aerospace Laboratory NLR, Rept. TP 2000-280, Amsterdam, 2000.

Acronyms

4D	4-Dimensional
ABRM	Analytic Blunder Risk Model
ADS-B	Automatic Dependent Surveillance-Broadcast
ASAT	Airspace Simulation and Analysis for Terminal instrument procedures
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
CCA	Common Cause Analysis
CDR	Conflict Detection and Resolution
CNS	Communication, Navigation and Surveillance
CRM	Collision Risk Model
DCPN	Dynamically Coloured Petri Net
ETA	Event Tree Analysis
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HMI	Human Machine Interface
HRA	Human Reliability Analysis
ICAO	International Civil Aviation Organisation
NASPAC	National Airspace Systems Performance Analysis Capability
NLR	Nationaal Lucht- en Ruimtevaartlaboratorium
PHA	Preliminary Hazard Analysis
RAMS	Reorganized ATC Mathematical Simulator
RASRAM	Reduced Aircraft Separation Risk Assessment Model
RNP1	Required Navigational Performance (95% of time within 1 n mile)
R/T	Radio Telephony
SDE	Stochastic Differential Equation
STCA	Short Term Conflict Alert
TAAM	Total Airspace and Airport Modeller
TCAS	Traffic alert and Collision Avoidance System
TOPAZ	Traffic Organization and Perturbation AnalyZer