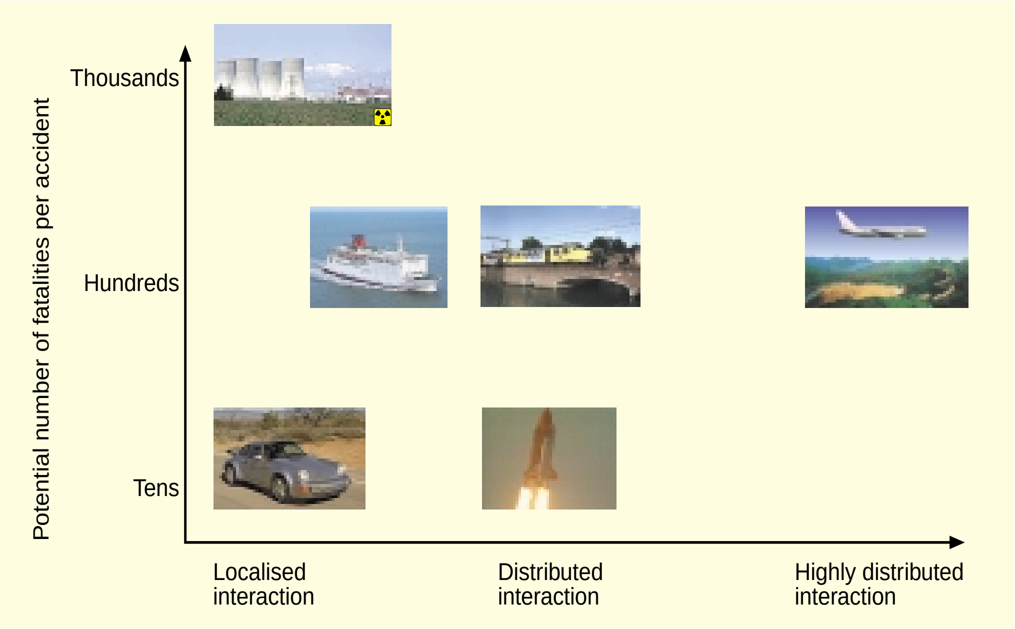
Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-99015

Accident risk assessment for advanced ATM

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-99015

Accident risk assessment for advanced ATM

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 a presentation held at the Second USA/Europe Air Traffic Management R&D Seminar, Orlando, 1-4 December 1998.

Division:	Air Transport
Issued:	January 1999
Classification of title:	unclassified

Summary

By now, safety is recognised as a key quality on which to select/design advanced 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 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 4D-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 highly distributed. This yields that providing safety is more than making sure that each of the ATM elements functions 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. In order 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 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.

Contents

7 Figures

(26 pages in total)

1 Introduction

ATM is the result of complex interactions between human operators, procedures and technical systems (hardware and software), all highly distributed. Providing safety is more than making sure that each of these elements functions properly safe. 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 with 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 organised around the clusters of individual elements, i.e. the communication cluster, the navigation cluster, the surveillance cluster, the automation tools cluster, the 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 that a costly development programme turns out ineffective, or that an even more costly implementation programme fails. Although understanding this idea is principally not very difficult, it can only be brought into practice when an ATM safety assessment approach is available that provides appropriate feedback to the ATM designers already at an early stage of the concept development (figure 1).

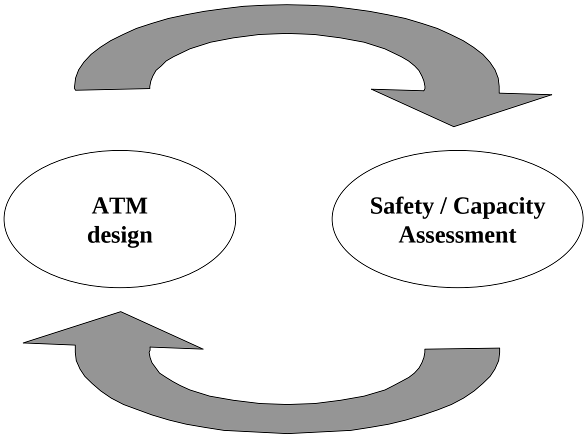


Fig. 1 Safety feedback based ATM design

This feedback should not only provide information on whether the design is safe enough, it should also identify the safety-capacity bottlenecks. By now, consensus is building that appropriate ATM safety modelling approaches are needed to understand the mechanisms behind designing advanced ATM. It is also recognised that, once such an ATM safety modelling approach is available, a safety feedback based design approach of future ATM will become feasible (Haraldsdottir et al., 1997; Odoni et al., 1997; EVAS, 1998).

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

- 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. Fact is that 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.
- 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. Randell, 1995; DAAS, 1995). However, they have been developed to cover technical systems only (e.g. SAE, 1994, 1995; EATCHIP, 1996), and not the human operators and procedures of ATM (Klompstra and Everdij, 1997).
- Accident risk (e.g. for 1st, 2nd and 3rd parties in air transport) metrics definitively are objective and are commonly in use for other human controlled safety-critical operations such as chemical and nuclear industries (Royal Society, 1983). Two well known ICAO adopted accident risk metrics are for collision of an aircraft with another aircraft during en-route phase, or with fixed obstacles during landing. A recent review of various accident risk metric possibilities in air transport is given in (Moek et al., 1997).

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 of 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 NASPAC, RAMS or TAAM fall short for that purpose. One major shortcoming of these tools is that they are not really capable of modelling 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 can not in a practically reasonable way be reached through a straightforward simulation, since this would require a simulation of 10^{10} aircraft flight hours. This problem is well illustrated by the ATM safety iceberg (figure 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, where 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.

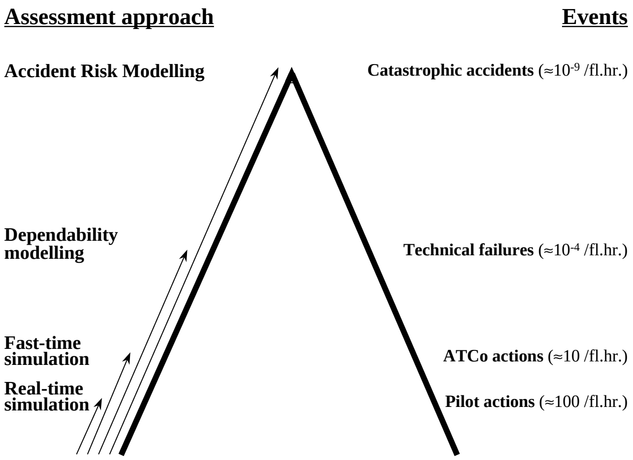

Assessment approach
Events
Accident Risk Modelling
Catastrophic accidents (≈10-9 /fl.hr.)
Dependability modelling
Technical failures (≈10-4 /fl.hr.)
Fast-time simulation
ATCo actions (≈10 /fl.hr.)
Real-time simulation
Pilot actions (≈100 /fl.hr.)

Fig. 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. In order 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 (Everdij et al., 1996a). 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 modelling, dynamic event trees, etc. (Aldemir et al., 1994). Each of these techniques has advantages and disadvantages, but these appear to be minor in comparison to what is required for modelling ATM related risk. The key finding is that the established techniques fail to support a systematic approach towards modelling stochastic dynamical behaviour over time for complex interactions of highly distributed ATM (see figure 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.

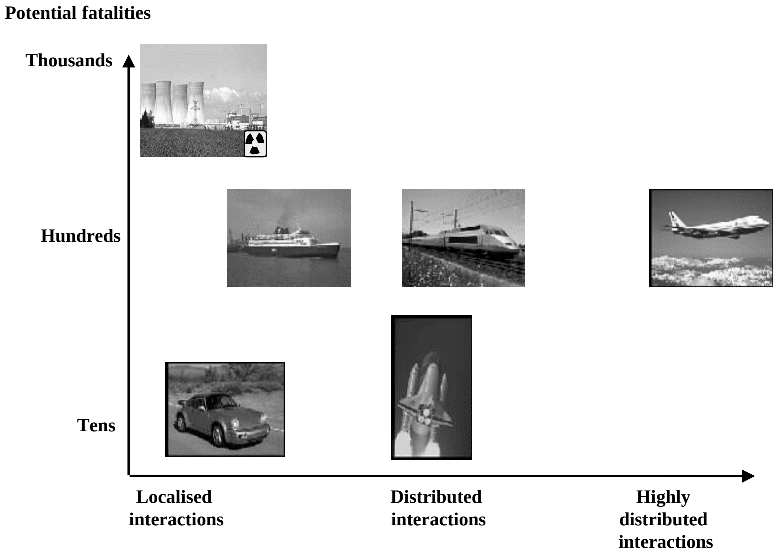


Fig. 3 Potential fatalities and distribution level of ATM and other safety critical activities.

The basic ATM safety assessment needs have already been identified in (Blom, 1992b). This finding motivated the development of an adequate safety assessment approach within a project named TOPAZ (Traffic Organization and Perturbation AnalyZer). The scientific basis for this was the idea to explore a stochastic analysis framework (Blom, 1990) which supports stochastic models where 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 mean time, from parallel conducted studies on advanced ATM it became crystal 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 (Blom and Bakker, 1993), 2) a stochastic dynamical game perspective (Blom et al., 1994) and 3) an ATM overall validation perspective (Blom et al., 1995).

The accident risk assessment results obtained through stochastic analysis studies have initially been exploited for an RLD/LVB project towards the assessment of accident risk for staggered landings on converging runways (Bakker et al., 1995; Everdij et el., 1996c). All this contributed to the development of both the TOPAZ assessment methodology, and a growing suite of TOPAZ 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 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 (Cohen et al., 1998). In addition to TOPAZ, four other collision risk directed approaches, ABRM, ASAT, ICAO's Collision Risk Model (CRM) and RASRAM (Sheperd et al., 1997), have been identified and reviewed; TOPAZ appeared to be most advanced in going beyond established approaches.

This paper is organised as follows. Section 2 gives an overview of the methodology. Next, section 3 outlines the principles of the underlying stochastic dynamical framework. Section 4 presents for several RNP1 example scenarios the results of TOPAZ based risk assessments. Section 5 gives concluding remarks on the methodology. The paper ends with references and acronyms.

2 The TOPAZ methodology

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

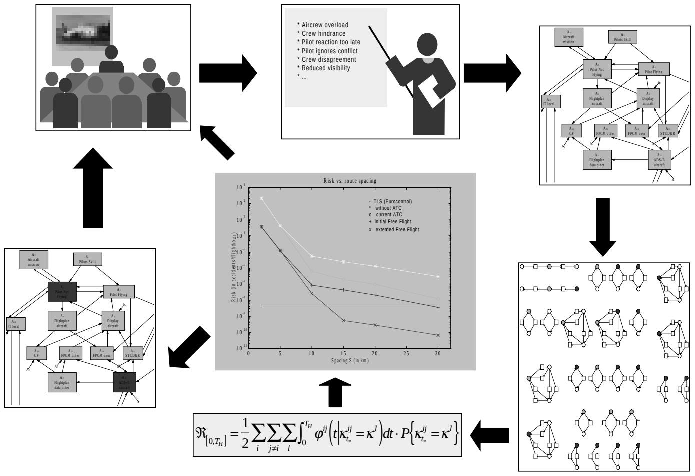


Fig. 4 TOPAZ assessment cycle

During such assessment cycle two types of assessments are sequentially conducted: first a qualitative safety assessment (illustrated by the upper drawings in figure 4), and then a quantitative safety assessment (illustrated by the middle and lower drawings in figure 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 data bases. The resulting list of identified potential hazards is subsequently analysed using established qualitative hazard analysis techniques in order 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 figure 4). Such modular representation is easily recognisable and understandable for ATM designers, thus supporting an effective communication between ATM designers and safety analysts.

From this point on, the TOPAZ assessment cycle continues with the quantitative phase, which is based on stochastic modelling, 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 fed back to the designers (see lower left corner of figure 4).

In order to form 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 others 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 TOPAZ modelling based improvement.

Underlying to a TOPAZ cycle there is a stochastic analysis framework, which allows to distinguish the following five activities:

a. Develop a stochastic dynamical model for the situation considered,
b. Where necessary develop appropriate cognitive models for human operators involved,
c. Perform the stochastic analysis necessary to decompose the risk assessment,
d. Execute the various assessment activities (e.g., through Monte Carlo simulation, numerical evaluation, mathematical analysis, or a combination of these),
e. Validation of the risk assessment exercise.

More details on these five activities are given below.

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 to aim 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. Elliott, 1982; Davis, 1984; Blom, 1990). 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 asks for 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 (Everdij et al., 1997b; Everdij and Blom, 1998), to which we refer as Dynamically Coloured 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 modelling

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 centred approach, in which unreliability is modelled through failures of human information processing, towards 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 (Amalberti and Wioland, 1997; Hollnagel, 1993; Bainbridge, 1993) that for the modelling 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 the in HRA widely used skill-, rule- and knowledge-based errors (Reason, 1990) essentially fall short to pay proper respect to, for example, situations where 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 up 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 sub-models for relevant operator actions that may blur understanding of how safety is achieved in ATM. In order 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., Biemans and Daams, 1997; Daams and Nijhuis, 1998). 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 (1993) with the Multiple Resources Theory of Wickens (1992), the classical slips/lapses model (Reason, 1990) and the human capability to recover from errors (Amalberti and Wioland, 1997). In addition, we have developed a model for the evolution of situational awareness errors. Compared with those considered in a recent study by (Hart et al., 1997), our approach shows to be an innovative one.

c. Perform stochastic analysis

Although it definitively is possible to realise a straightforward Monte Carlo simulation of the SDE model, it will be clear from the earlier discussion that this will not be really effective for the assessment of catastrophic risks in aviation. In order to develop an effective approach to the numerical evaluation of an SDE model, the SDE should be analysed 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 analyse 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 appeared to work satisfactorily for all situations evaluated.

d. Execute the various assessment activities

Typically, the resulting sequence of conditional assessments reads 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 analyses 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 analyser.
6. Transform all results from the preceding conditional assessments into appropriate safety metrics.

7. Identify the safety-separation and/or safety-modelling bottlenecks, of the specifically modelled ATM concept/scenario.

For each of these activities, except 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. In order to handle this in a valid way, we make use of a mathematical framework, the basis of which is explained in section 3.

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. Due to our underlying stochastic analysis framework, such a validation can be done through executing the following activities:

- 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.
- Verify the correctness of the instantiated DCPN versus the results of the qualitative assessment and the assumptions adopted. This should be done by stochastic analysis TOPAZ experts, with at least one who has not been involved with the DCPN instantiation.
- 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.
- 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.

3 The mathematical framework

Each DCPN instantiation can be represented by an SDE on a hybrid state space (Everdij and Blom, 1998), 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:

$$\tfrac{d}{dt} p_{\xi_t}(\xi) = \mathcal{L} p_{\xi_t}(\xi)$$

with $\mathcal{L}$ an operator defined by the Markov process $\{\xi_t\}$. Due to 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):

$$\tfrac{d}{dt} p_{\xi_{t|\tau}}(\xi) = \mathcal{L} p_{\xi_{t|\tau}}(\xi), \text{ for } t > \tau.$$

It is particularly relevant to notice that the above equations are well known for Markov chains, i.e. Markov processes with discrete state space, which processes have shown to be very useful in the development of advanced dependability and performability assessment methodology (e.g. Pattipati et al., 1993; Fota et al., 1997). For hybrid state Markov processes, this equation is well known in Bayesian estimation theory (e.g. Blom, 1990) and this has a.o. led to advanced multi target multi sensor tracking applications (e.g. Blom et al., 1992a).

The above 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 3D location and 3D velocity of aircraft i, $i \in \{1, \ldots, n\}$. Let $y_t^{ij} \overset{\Delta}{=} y_t^i - y_t^j$, let $v_t^{ij} \overset{\Delta}{=} v_t^i - v_t^j$ 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 say an incrossing occurs, and each time the process $\{y_t^{ij}\}$ leaves the area D^{ij}, we say 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 (Bakker and Blom, 1993) the expected number $\mathcal{R}_{[0,T]}$ of incrossings, or collisions, between aircraft pairs in the time-interval $[0, T]$ satisfies:

$$\mathcal{R}_{[0,T]} = \sum_{i=1}^{n} \sum_{j>i}^{n} \int_0^T \varphi^{ij}(t)\, dt$$

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

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

In (Bakker and Blom, 1993) 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 characterisation 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 above equations can be transformed into:

$$\mathcal{R}_{[0,T]} = \sum_{i=1}^{n} \sum_{j>i}^{n} \sum_{\kappa} \int_{\tau^{ij}}^{T} \varphi^{ij}(t \mid \kappa_{\tau^{ij}}^{ij} = \kappa)\, dt \;\cdot P\{\kappa_{\tau^{ij}}^{ij} = \kappa\}$$

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

$$\varphi^{ij}(t \mid \kappa_{\tau^{ij}}^{ij} = \kappa) \stackrel{\Delta}{=} \lim_{\Delta \downarrow 0} P\{y_t^{ij} \notin D^{ij}, y_{t+\Delta}^{ij} \in D^{ij} \mid \kappa_{\tau^{ij}}^{ij} = \kappa\}/\Delta$$

In figure 5, the equation for $\mathcal{R}_{[0,T]}$ is presented in the form of a tree, in which $f^{ij}(\kappa)$ is short for $\int_{\tau^{ij}}^{T} \varphi^{ij}(t \mid \kappa_{\tau^{ij}}^{ij} = \kappa)\, dt \cdot P\{\kappa_{\tau^{ij}}^{ij} = \kappa\}$. This tree has some resemblance with the well known fault tree. However, due to the underlying stochastic and physical relations, our new tree differs significantly and is named Collision Risk Tree.

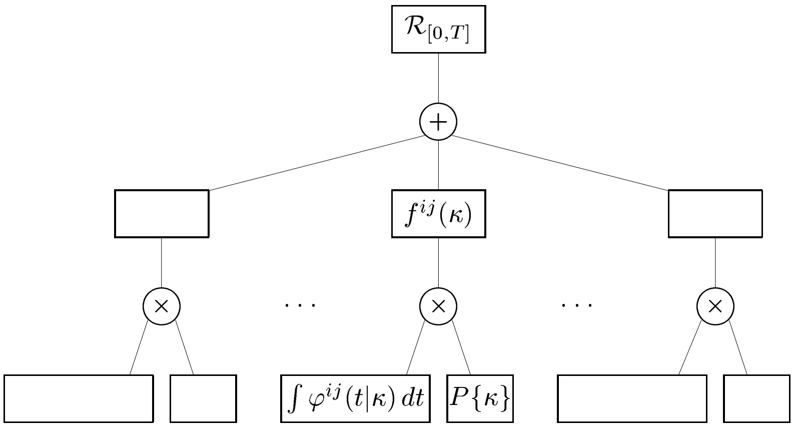


Fig. 5 Collision Risk Tree

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

- Monte Carlo simulations of the DCPN to quantify $P\{\kappa^{ij}_{\tau^{ij}} = \kappa\}$ and the statistical properties of the relevant DCPN components at the stopping time τ^{ij}.
- Evaluations of the evolution of the relative aircraft states from stopping time τ^{ij} on, and for each $\kappa^{ij}_{\tau^{ij}} = \kappa$. If complexity requires, this process can even be done for a sequence of increasing stopping times.
- Numerical evaluation of $\int_{\tau^{ij}}^{T} \varphi^{ij}(t \mid \kappa^{ij}_{\tau^{ij}} = \kappa)\, dt$, using the Generalized Reich equation of (Bakker and Blom, 1993), see also (Kremer et al., 1998).

4 RNP1 in conventional and airborne separation assurance scenario examples

In this section, the TOPAZ approach is used to evaluate a simple scenario of two en-route traffic streams of RNP1 equipped traffic, flying in opposite direction, all at one single flight level. This rather hypothetical scenario has been developed by Eurocontrol with the aim to learn understanding 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 (Everdij et al., 1997a):

- Straight route, with two traffic lanes (figure 6),
- Flight plans contain no lane changes
- Parameter S denotes distance between the two lanes,
- Opposite traffic flows along each lane,
- Aircraft fly at one flight level only
- Traffic flow per lane is 3.6 aircraft/hour,
- All aircraft nominally perform RNP1,
- None of the aircraft are TCAS equipped,
- Target level of safety is $5 \cdot 10^{-9}$ accidents/flight hour.

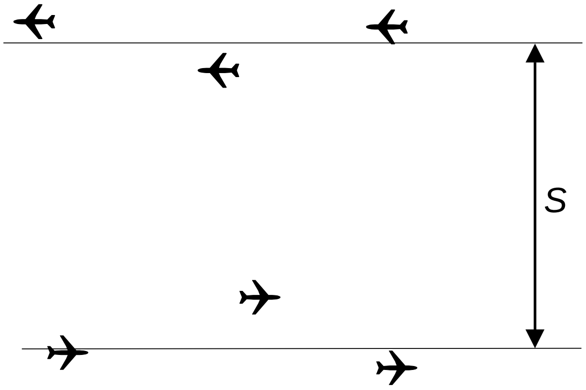


Fig. 6 Opposite direction traffic in a dual lane route

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

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

B) STCA-only based ATC. In this case there is radar based surveillance and 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 ATCo. It should be noticed that this differs significantly from conventional ATC, where an executive controller autonomously monitors and issues corrective actions, while STCA is a safety net only.

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

D) Negotiated airborne separation assurance, a design that is explicitly due to the feedback received from TOPAZ based safety assessments conducted for A), B) and C). For this concept it is assumed that aircraft also behave co-operatively 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 five minutes 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 learn understanding 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 TOPAZ methodology and tool set have been used to conservatively assess accident risk for the above scenario, as a function of the spacing parameter S. The resulting accident risk curves are presented in figure 7. Since all four curves are based on conservative modelling assumptions for the ATM situations considered, they provide an upper bound for the true accident risk.

These results are obtained over a period of two years during three subsequent studies. The first en-route study (Everdij et al., 1997a) 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 TOPAZ methodology. Concept B) has been assessed during an initial study for Eurocontrol (Everdij et al., 1997). Concept C) has been developed (Hoekstra et al., 1997) and assessed (Daams et al., 1997) during studies within NASA's Free Flight research programme. The safety assessment results from concepts A), B) and C) have subsequently been fed back (Van Gent et al., 1997) to enable the safety based design concept D), and subsequently to assess it with TOPAZ (Daams et al., 1998).

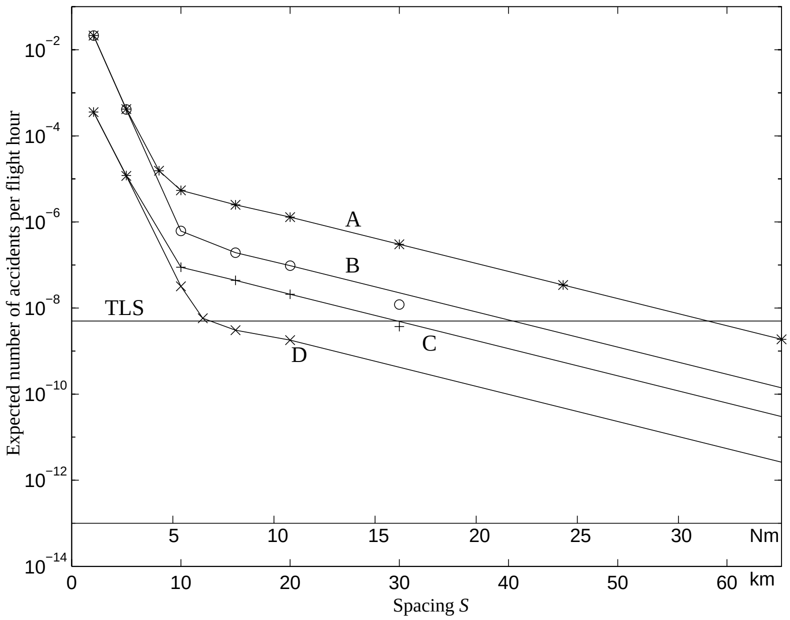


Fig. 7 Accident risk for the opposite traffic scenario, as a function of spacing parameter S, for the four ATM concepts considered: A) Procedural separation, B) STCA-based ATC, C) Basic airborne separation assurance, D) Negotiated airborne separation assurance. The accident risk unit used is from ICAO,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

The risk curves in figure 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 NM, 22 NM, 16 NM and 7 NM for ATM concepts A), B), C) and D) respectively. The large value of 31 NM for concept A) does not come as 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 net which 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 co-operative 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-a/c), while for the co-operative airborne-based concept C) each of the two encountering aircraft has a monitoring and decision-making loop (surveillance-CDR-pilot-a/c) 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 NM to 16 NM. 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 NM and 16 NM, concepts B) and C) do not support spacings that are required for busy fixed route situations over the continent.

Finally, the co-operative Negotiated airborne separation assurance concept D) allows such low spacing values. This is not a coincidence, but the result of effectively making use of TOPAZ based safety feedback from A), B) and C). It appeared that for all these three 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 TLS. To accomplish this, the two monitoring and decision-making loops of concept C) have been extended with a largely independent and co-operative 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.

5 Concluding remarks

This paper has given an outline of the TOPAZ methodology to assess advanced ATM on mid-air 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:

- It applies established techniques during a qualitative assessment phase only;
- Quantification is based on stochastic dynamical modelling;
- Uses powerful tools from the theory of stochastic analysis;
- Handles complex interactions between different ATM elements;
- Incorporates advanced human cognitive modelling;
- Incorporates the Generalized Reich collision risk model;
- Provides effective feedback to ATM concept designers;
- 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 optimisation 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 of section 4 can relatively simply be extended to other encounter scenarios. This also means that it should be possible to identify classes of encounter scenarios such that it is sufficient to perform an accident risk assessment for one scenario from each class only.

In this paper the TOPAZ methodology has been concentrated on the risk of mid-air collision. Due to the generality of the methodology, however, we believe 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 TOPAZ methodology with a probabilistic model for wake vortex induced accident risk (Blom and Speijker, 1998).

6 References

1. T. Aldemir, N.O. Siu, A. Mosleh, P.C. Cacciabue and B.G. Göktepe (Eds.) Reliability and safety assessment of dynamic process systems, Springer, 1994.
2. R. Amalberti and L. Wioland, Human error in aviation, In: Aviation safety, pp. 91-108, H. Soekkha (Ed.), 1997.
3. L. Bainbridge, The change of concepts needed to account for human behaviour in complex dynamic tasks, Proc. 1993 Int. Conf. on Systems, Man and Cybernetics, pp. 126-131, 1993.
4. G.J. Bakker and H.A.P. Blom, Air Traffic Collision risk modelling, Proc. 32nd IEEE Conf. on Decision and Control, pp. 1464-1469, 1993.
5. G.J. Bakker, H.A.P. Blom and M.H.C. Everdij, Collision risk evaluation of the dependent converging instrument approach (DCIA) procedure under Gaussian deviations from expected missed approach paths, NLR report CR 95322 L, 1995.
6. M.C.M. Biemans and J. Daams, Human Operator Modelling to Evaluate Reliability, Organisation and Safety, NLR report TR 98073, 1997.
7. H.A.P. Blom, Bayesian estimation for decision-directed stochastic control, Ph.D. thesis, Delft University of Technology, 1990.
8. H.A.P. Blom, R.A. Hogendoorn and B.A. Van Doorn, Design of a multisensor tracking system for advanced air traffic control, Ed: Y. Bar-Shalom, Multitarget-Multisensor Tracking, Volume II, Artech House, pp. 31-63, 1992a.
9. H.A.P. Blom, The layered safety concept, an integrated approach to the design and validation of air traffic management enhancements, NLR report TP 92046 L, 1992b.
10. H.A.P. Blom and G.J. Bakker, A macroscopic assessment of the target safety gain for different en-route airspace structures within SUATMS, NLR report CR 93364 L, 1993.
11. H.A.P. Blom, M.B. Klompstra and G.J. Bakker, Air Traffic Management as a multi-agent stochastic dynamic game under partial state observation, Proc. IFAC Symp. Transportation Systems, 1994, Tianjin, pp. 249-254.
12. H.A.P. Blom, C.F.W. Hendriks and H.B. Nijhuis, Assess necessary validation developments, VAPORETO WP3 final report, NLR report CR 95524 L, 1995.
13. H.A.P. Blom and L.J.P. Speijker, NLR's initial probabilistic wake vortex model for TOPAZ, NLR draft report, September 1998.
14. S. Cohen et al., A concept paper for separation safety modelling, FAA/Eurocontrol, May 1998.
15. J. Daams, G.J. Bakker and H.A.P. Blom, Safety evaluation of an initial free flight scenario with TOPAZ, NLR report TR 98098, 1998a.

16. J. Daams, G.J. Bakker and H.A.P. Blom, Safety evaluation of encounters between free-flight equipped aircraft in a dual route structure, NLR report, forthcoming, 1998b.
17. J. Daams and H.B. Nijhuis, Human Operators Controllability of ATM safety, ARIBA, NLR final report, forthcoming, 1998.
18. DAAS (Dependability Approach to ATM Systems), Work package reports for the European Commission DG XIII, 1995.
19. M.H.A. Davis, Piecewise Deterministic Markov Processes: a general class of non-diffusion stochastic models, J. Royal Statist. Soc. (B), Vol 46, pp. 353-388, 1984.
20. EATCHIP, Air Navigation System Safety Methodology, Eurocontrol, Edition 0.4, Working Draft, 1996.
21. R.J. Elliott, Stochastic calculus and applications, New York, Springer, 1982.
22. EVAS, EATMS Validation Strategy Document, Edition 1.1, Eurocontrol, June 1998.
23. M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom and O.N. Fota, Evaluation of hazard analysis techniques for application to en-route ATM, MUFTIS Final Report on Safety Model, Part I, NLR report TR 96196 L, 1996a.
24. M.H.C. Everdij, M.B. Klompstra and H.A.P. Blom, Development of mathematical techniques for ATM safety analysis, MUFTIS Final report on Safety model, Part II, NLR report TR 96197 L, 1996b.
25. M.H.C. Everdij, G.J. Bakker and H.A.P. Blom, Application of Collision Risk Tree Analysis to DCIA/CRDA through support of TOPAZ, NLR report CR 96784 L, 1996c.
26. M.H.C. Everdij, G.J. Bakker, H.A.P. Blom and P.J.G. Blanker, Demonstration report in preparation to Designing EATMS inherently safe, TOSCA II WP4 phase I report, NLR, 1997a.
27. M.H.C. Everdij, H.A.P. Blom and M.B. Klompstra, Dynamically Coloured Petri Nets for Air Traffic Management Safety purposes, Proc. 8th IFAC Symposium on Transportation Systems, pp. 184-189, 1997b.
28. M.H.C. Everdij and H.A.P. Blom, Piecewise Deterministic Markov Processes represented by Dynamically Coloured Petri Nets, Submitted, 1998.
29. N. Fota, M. Kaaniche and K. Kanoun, A modular and incremental approach for building complex stochastic Petri net models. Proc. First Int. Conf. on Mathematical Methods in Reliability, 1997.
30. A. Haraldsdottir et al., Air Traffic Management Concept Baseline Definition, NEXTOR Report RR-97-3, Boeing, 1997.
31. S. Hart et al. A designers guide to human performance modelling, AGARD AMP Working Group 22 draft report, 1997.
32. J.M. Hoekstra, R.C.J. Ruigrok and R.N.H.W. van Gent, Conceptual design of Free Flight Cruise with Airborne Separation Assurance, NLR report TP 98252, 1997.

33. E. Hollnagel, Human Reliability analysis, context and control. Academic Press, London, 1993.
34. M.B. Klompstra and M.H.C. Everdij, Evaluation of JAR and EATCHIP safety assessment methodologies, NLR report CR 97678 L, 1997.
35. H.J. Kremer, G.J. Bakker and H.A.P. Blom, Geometric and probabilistic approach towards conflict prediction in free flight, forthcoming, 1998.
36. G. Moek, M.B. Klompstra, H.A.P. Blom et al., Methods and Techniques, GENOVA Final Report, NLR, 1997.
37. A.R. Odoni et al., Existing and required modeling capabilities for evaluating ATM systems and concepts, Final report, MIT, March 1997.
38. K.R. Pattipati, Y. Li, and H.A.P. Blom, A unified framework for the performability evaluation of fault-tolerant computer systems, IEEE Transactions on Computers, Vol. 42 (1993), pp. 312-326.
39. B. Randell (Ed.), Predictably dependable computing systems, Springer, 1995.
40. J. Reason, Human error, Cambridge Univ. Press, 1990.
41. Royal Society, Risk assessment, report of a Royal Society Study Group, 1983
42. SAE, 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.
43. SAE, 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.
44. R. Sheperd, R. Cassell, R. Thava and D. Lee, A reduced aircraft separation risk assessment model, Proc. AIAA Guidance, Navigation and Control Conf., New Orleans, August 1997.
45. R.N.H.W. Van Gent, J.M. Hoekstra and R.C.J. Ruigrok, Free Flight with Airborne Separation Assurance, Proc. CEAS symposium, October 1997, Amsterdam.
46. C.R. Wickens, Engineering, psychology and human performance, Merrill, 1992

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
NM	Nautical Mile
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 NM)
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