Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2006-695

Modelling lateral spacing separation for airborne separation assurance using Petri nets

M.H.C. Everdij, H.A.P. Blom and G.J. Bakker

This report contains a paper to appear in Simulation; Transactions of the Society for Modelling and Simulation International.

This report may be cited on condition that full credit is given to NLR and the authors.

Customer:	National Aerospace Laboratory NLR
Working Plan number:	2005 AT.1.A
Owner:	National Aerospace Laboratory NLR
Division:	Air Transport
Distribution:	Unlimited
Classification title:	Unclassified
	September 2006

Approved by:

Author	Reviewer	Managing department
ME'06	Anonymous peer reviewers	22/12/06

MODELLING LATERAL SPACING AND SEPARATION FOR AIRBORNE SEPARATION ASSURANCE USING PETRI NETS

Mariken H.C. Everdij, Henk A.P. Blom, and Bert G.J. Bakker,

National Aerospace Laboratory NLR, Amsterdam, The Netherlands,

everdij@nlr.nl; blom@nlr.nl; bakker@nlr.nl

Abstract

Airborne separation assurance is seen as a promising option for the future air traffic management concept to provide an increase in capacity and flight efficiency while maintaining flight safety. Sofar, studies or expectations are largely based on assumptions about the achievable spacing and separation criteria. These assumptions range from optimistic to reserved, when comparing these separation criteria to currently used radar surveillance-based values. In any case, there is a clear knowledge gap on this subject. Thus, it is important to assess the relationship between spacing and separation distances on one hand and safety on the other hand. This relationship directly affects the effectiveness of airborne separation assurance.

The aim of this paper is to address this issue by conducting an accident risk assessment, including a bias and uncertainty assessment and an assessment of risk sensitivity to spacing and separation values. Each stage in the methodology used is illustrated by examples. It is shown that the methodology provides valuable feedback on both the airborne separation assurance operation and the accident risk assessment.

1. Introduction

This paper estimates a difficult metric, namely the risk of the rare event of collision between two aircraft under a concept of operation that does not yet exist in any aviation system worldwide but has been proposed as a viable alternative for the future.

Rare event estimation has been widely studied for various safety-critical operations, such as the nuclear and chemical industries, air traffic and many other. Rare event estimation approaches can be subdivided into two groups: approaches based on statistical analysis of collected data and those that are based on the modelling of the processes leading to the accident. The statistical analysis of extreme values needs a long observation time given the very low probability of the events considered, [1]. The modelling approach consists of formulating the operation considered and secondly by using Petri net modelling, analysis and simulation in obtaining rare event estimates, [2], [3].

The approach used in this paper is a good example of the latter approach to estimate such a difficult metric of collision risk between aircraft and yet retrieve practical results. The salient feature of modelling this risk is that multiple non-nominal events must occur for such a collision to happen. As such, modelling these events is critical, and this paper exploits the use of Petri Nets and state-based Monte Carlo simulation as a good technique for this type of analysis.

2. Concept operation to be modelled

By exploiting advances in flight deck technologies, such as ADS-B (Airborne Dependent Surveillance - Broadcast), and air-to-air data link, airborne separation assurance is seen as a promising option for the future Air Traffic Management (ATM) concept, to provide an increase in capacity and flight efficiency while maintaining flight safety. In this concept, pilots are allowed to select their trajectory freely at real time, at the cost of acquiring responsibility for conflict prevention [4], [5]. It changes ATM in such a fundamental way, that one could speak of a paradigm shift: the centralised control becomes a distributed one, responsibilities transfer from ground to air, air traffic control sectorisation and routes are removed and new technologies are brought in. It also plays an important role in the distributed air-ground traffic management concept, which allows for distributed decision-making between flight deck, air traffic service providers and aeronautical operational control centres of airlines, for further optimisation of operations.

The advantage of airborne separation assurance is that it may eliminate the situation that acceptable ground controller workload puts a limit on air traffic capacity. Hence, an alternative operational concept worth investigating is one in which there is no tactical air traffic controller; all separation assurance tasks lie with the pilots. The general expectation is that with such a concept, air traffic capacity may

improve significantly, even if spacing and separation criteria would stay the same. At the same time, it is generally accepted that a particular airborne separation assurance based operational concept will have its own capacity/safety limitations. Hence, many studies or expectations are based on particular hypotheses about the achievable spacing or separation criteria. Optimistic views are that they could be much smaller than radar separation; other views are much more reserved and warn that minimum separation distances might be much larger. In any case, there is a clear knowledge gap on this subject. Thus, it is important to assess the relationships of spacing between flight plans, separation between airpaths, and collision risk, as they directly affect the effectiveness of an airborne separation assurance application, [6].

Since collisions occur very infrequently, even for current ATM procedures there is not sufficient statistical data to verify evaluated collision risk results in a direct way against operational data. For new operations, such as autonomous (i.e. free flight) aircraft operations, there even is far less operational data available. Therefore, one has to rely on model-based risk assessment to gain insight into this complex matter. It can help to learn where unsafety comes from, how it is influenced, which factors have the highest impact, and what contribution is coming from separation distances.

3. Approach taken

In 1998, by a joint effort of Eurocontrol and FAA, in collaboration with some key developers of aviation risk assessment tools, an overview was produced [7] that outlines the relevant approaches in development and/or in use for the safe separation assessment of advanced procedures in air traffic. Five collision risk directed approaches, i.e. ABRM (Analytic Blunder Risk Model) [8], ASAT (Airspace Simulation and Analysis for Terminal instrument procedures), the Collision Risk Model (CRM) of ICAO (International Civil Aviation Organisation) [9], RASRAM (Reduced Aircraft Separation Risk Assessment Model) [10], and TOPAZ (Traffic Organisation and Perturbation AnalyZer) [11] were identified and reviewed. The TOPAZ methodology appeared to be most advanced in adopting a simulation model-based risk assessment and in going beyond established approaches. Since then, TOPAZ has been further extended, e.g. by a bias and uncertainty assessment method [12].

In this paper, we present the results obtained by a TOPAZ based accident risk assessment for a hypothetical situation in which aircraft equipped for free flight are assumed to maintain separation without direct involvement of Air Traffic Control (ATC). For the accident risk assessment, we consider the flow of traffic between two major airports only, say A and B, and assume that the aircraft fly on a direct route between these two airports, separated on two parallel opposite direction lanes at the same flight level, see Figure 1. In this figure, *S'* denotes lateral separation minimum and *S* denotes lateral spacing between the parallel opposite direction lanes. If the spacing *S* is taken to be equal to or smaller than the separation minimum *S'*, it would be quite likely that two aircraft on two opposite direction lanes often need to manoeuvre in order not to lose minimum separation. Hence, an effective safe spacing level for *S* should at least be larger than a safe separation minimum *S'*. Both for *S* and *S'*, it is important to further learn understanding what criteria should apply. Obviously, in a full free flight situation, there are many other encounter types that have to be studied (crossing routes, cross flight level, join same flight level, longitudinal separation, etc.). The idea is to understand the relation between accident risk and lateral spacing for one encounter type first, before proceeding to study other encounter types.

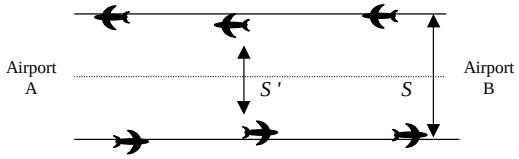

Figure 1: Top view of two opposite direction parallel lanes at the same flight level. *S* denotes lateral spacing, *S'* denotes lateral separation minimum.

The objective of this paper is to estimate safe values for *S* and *S'*, for a stream of aircraft that are all equipped according to the free flight operational concept outlined in Section 5. The safe spacing evaluation of opposite traffic streams within this operational concept is performed through an organised sequence of well-defined accident risk assessment stages:

1. Identify the operation to be assessed.
2. Identify all hazards.
3. Instantiate a mathematical model for the operation to be assessed.
4. Perform an accident risk assessment for this mathematical model of the operation.
5. Assess risk bias and uncertainty due to differences between the mathematical model and the real operation considered.
6. Compare the assessed accident risk levels with applicable risk criteria and evaluate the impact of separation criteria.
7. Assess the safety and spacing critical elements of the operation considered.

For the application considered in this paper, stages 1, 2, 3 and 4 have been executed in [13]; stages 5, 6 and 7 have been executed in [14]. The main results of all stages are presented in this paper.

The paper is organised as follows: Section 4 presents the results of stage 1 (operation). Section 5 presents the results of stage 2 (hazards). Section 6 presents the results of stage 3 (instantiate model). Section 7 presents the results of stage 4 (model-based risk assessment). Section 8 presents the results of stages 5 and 6 (bias and uncertainty assessment and impact of separation criteria). Section 9 presents the results of stage 7 (critical elements of operation). Section 10 draws conclusions.

4. Operational concept considered

The separation assurance equipment of the aircraft considered is based on an extension of an Initial Free Flight (IFF) operational concept developed by Hoekstra *et al* [15], which is one of the various free flight operational concepts developed [16]. Based on the IFF accident risk assessment results [17], operational concept extensions have been developed, leading to the Extended Free Flight (XFF) operational concept. The main characteristics of XFF are as follows:

- Aircraft are equipped with ADS-B, and use this to inform other aircraft about both their position/speed and their intent (flight plan).
- Aircraft have medium term conflict detection and resolution (CD&R) automation support that detects conflicts between flight plans and proposes a flight plan resolution.
- Aircraft have Flight Plan Conformance Monitoring (FPCM) that detects severe deviations by both the own and the other aircraft from their respective flight plans and proposes a flight plan adjustment to increase separation.
- Aircraft have short term CD&R automation support that detects conflicts and gives resolution advisories, which the pilots can confirm and then automatically fly.

Some additional explanation is given in subsections 4.1 through 4.9.

4.1 Airspace organisation

The airspace is not covered by radar and is without any ATC separation support. Aircraft are expected to fly direct routes between entry and exit points, conform the agreed plan with air traffic flow management (ATFM). In this paper, the collision risk analysis is subsequently limited to one of these direct routes, with two opposite direction parallel lanes at the same flight level (Figure 1). Hence, it is assumed that nominally the aircraft flight plan is conform the ATFM agreed plan, i.e. conform the right lane.

4.2 ADS-B

ADS-B is used to inform other aircraft of aircraft state (position and speed vector) and intent (flight plan) information. In flight, each aircraft broadcasts at an update rate of one per second nominally:

- the medium term flight plans (available in FMS),
- the own state estimates (available from its navigation system).

Hence, the following information is available on board of each aircraft:

- The flight plan of the own aircraft.
- The estimated state of the own aircraft.
- The medium term flight plans of the surrounding aircraft (say, within 60 Nm radius).
- The state estimate information from the surrounding aircraft.

4.3 Medium term CD&R

Conflict Probing (CP) checks whether the flight plans of the own aircraft and the surrounding aircraft (which are available through ADS-B) are in conflict (i.e., distance smaller than S', see Figure 1) in medium term, and proposes a flight plan resolution. This is done on board of each aircraft, by testing whether a conflict between flight plans occurs within medium term (i.e. the next 5 minutes). If a conflict between flight plans is detected, the pilots-not-flying of the aircraft involved are both alerted through their displays upon which they both have the responsibility to adjust their flight plans by confirming the proposed resolution to increase separation (minimally S between the flight plans). Normally, only one aircraft adjusts his flight plan in response to the alert. The reason for this is that it takes some time before proper action is taken: if one aircraft adjusts his flight plan such that there is no conflict, there is no reason for the other aircraft to adjust his flight plan.

4.4 FPCM

The FPCM monitors whether the aircraft evolutions of both the own and the surrounding aircraft conform to their flight plans. This is done on board of each aircraft, by comparison of the aircraft filtered state and the flight plan for each aircraft. If the deviations between the aircraft filtered state and the flight plan are severe, i.e. pass a given threshold (taken about 1.5 Nm), then the pilots-not-flying are alerted through their display. Also, a flight plan resolution is automatically proposed.

- If the FPCM alert concerns a severe deviation of some nearby aircraft from its flight plan, the

pilot-not-flying (i.e. the pilot who is not actively flying the aircraft, but who has other tasks such as communication) has the task to adjust the flight plan of his own aircraft by confirming the proposed resolution to increase separation (minimally 10 Nm between the flight plans) with the deviating aircraft.

- If the FPCM alert concerns a severe deviation from the aircraft's own flight plan, the pilot-not-flying has the responsibility to advice the surrounding aircraft through R/T to increase the minimal separation between flight plans to minimally 10 Nm and to ask the pilot-flying to return to flight plan. Furthermore, the pilot-not-flying tries to solve the problem that caused the severe deviation. If necessary, the pilot-not-flying of another aircraft will adjust his flight plan to ensure this separation.

Adjustments in flight plan to ensure sufficient separation by deviating aircraft are assumed to consist of an immediate turn to the left or to the right, which heading is flown until the original heading can be resumed without compromising the desired separation between flight plans. If the point of closest approach is passed, each aircraft returns to its original flight plan. For the same reason as with medium term CD&R: normally, only 1 aircraft will adjust his flight plan.

4.5 Short term CD&R

The pilots of both conflicting aircraft are warned automatically if a separation conflict (i.e., distance smaller than *S'*, see Figure 1) is expected to occur within 2 minutes on the basis of the neighbouring aircraft's estimated position and velocity vectors (which are available through ADS-B) and the predicted position and velocity (using linear prediction). After detection, a conflict resolution is proposed automatically for each aircraft using the Voltage Potential algorithm (see [15]) which proposes adjustments in the horizontal velocities (with no priority rules). After some human response time the pilot-flying confirms the proposed conflict resolution. Then the resolution is carried out automatically and is continuously updated (every 10 seconds) effectively according the state estimate update without further pilot acknowledgements. Hence, normally, both aircraft will perform conflict resolution.

4.6 Priority rules in reacting to alerts

The following rules determine the priority of reacting to alerts:

- Short term conflict detection and resolution is handled with priority over CP or FPCM alerts. The underlying reason is that in case of a short term conflict, immediate action is required, whereas CP and FPCM alerts require action at planning level.
- If both CP and FPCM issue an alert, the FPCM alert is handled with priority. The underlying reason is that the aircraft that causes the FPCM alert cannot be expected to take effective action to ensure separation, since the pilots on board are probably preoccupied with repairing the problem that caused the alert. This is in contrast to the case of a CP alert, where it is reasonable to assume that the other aircraft will also taken action.
- An FPCM alert concerning the own aircraft has priority over FPCM alerts concerning other aircraft. This is due to the observation that in case that the own aircraft cannot adhere to the flight plan very well, adjustments of the flight plan to avoid some other aircraft are not expected to be very effective. Therefore, priority lies with warning the other aircraft (in case they have not detected the deviation themselves yet) and solving the problem on board.

4.7 XFF-specific human responsibilities

The general responsibilities of the pilot-flying and the pilot-not-flying are to carry out the mission of the aircraft in a safe and efficient manner. The XFF-specific responsibility of the pilot-flying is the correct execution of the flight plan. The responsibility of the pilot-not-flying is to respond to any CD&R automation messages by looking at the CD&R traffic screen and taking appropriate actions. It is assumed that the pilots do not take over each other's role. ATC is only involved when an aircraft leaves or enters the free flight airspace considered.

4.8 Radio communication

For emergency situations (e.g. to warn other aircraft in case of severe deviations from flight plan due to aircraft system problems), the pilots-not-flying have radio only to communicate with each other.

4.9 Navigation

Aircraft navigation performance is assumed to be RNP1 (Required Navigation Performance), which means that an aircraft stays within ± 1 Nm of its flight plan for 95% of the time. Ground navigation support is VOR/DME (Very high frequency Omni-directional Range/ Distance Measuring Equipment; this is navigation based on ground beacons).

5. Hazard identification

Once the operational concept has been sufficiently described (note that this does not mean that too much detail is required or called for, such as air temperature or specific route coordinates), the hazards are identified. This is done in two steps: (1) Identification of entities and their functional relationships; (2) Identification of hazards, both functional and non-functional.

5.1 Identification of entities

In this step, the operational concept description is investigated to identify the entities of the operation. These entities may be humans (pilot-flying; pilot-not-flying), technical systems (navigation support; ADS-B; cockpit display; FPCM, etc.), or even more abstract entities (e.g. pilot training; weather; aircraft mission; aircraft evolution). For XFF, the complete list is provided in [13]. The main entities for XFF are also given in Figure 2, each represented by a box, and dependency relations are represented by arrows between the boxes.

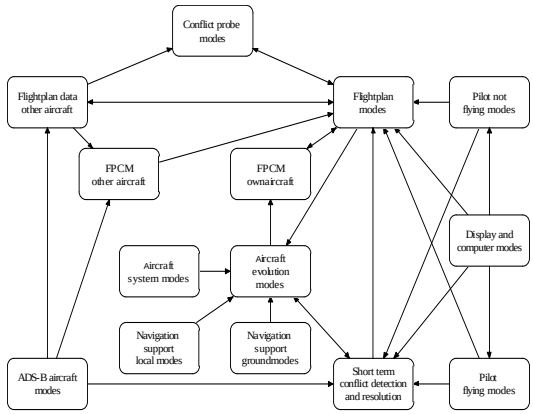

Figure 2: Functional dependency relations between the main entities for XFF.

5.2 Identification of hazards

This step involves the identification of as many hazards that may occur during the XFF operation as possible. Several systematic techniques exist that can be used for this task. Many of these techniques can be used to identify *functional hazards*, i.e. hazards that can be derived from the functional representation adopted in Figure 2. Examples of such functional hazards are: Navigation system failure; Pilot fails to make turn; Corrupted ADS-B data sent. More demanding to identify are the *non-functional hazards*, which are mostly human-related. These hazards are best identified using dedicated brainstorm sessions with a few participants bringing complementary expertise, for example one experienced pilot and one experienced air traffic controller. An additional important source of hazards is hazard databases.

For XFF, about 230 hazards have been identified; the list is provided in [14]. Of these, about 46% is of technical system nature. About 36% is human related, about 13% is procedure-related, and the remaining hazards are of other nature (e.g. weather). A list of some non-functional hazards is given in Table 1.

Table 1: Some non-functional hazards identified for XFF.

Id	Hazards
M3	Two aircraft do not detect conflict at the same time
M5	Pilot solves a conflict that occurs later than the cockpit display look-ahead time
M6	Pilot does not know whether other aircraft has conflict displayed
M18	Old intent data is transmitted because pilot has no time to update FMS during emergency
M34	Aircrew unaware of loss of communication (think it's just quiet)
0473	Pilot does not acknowledge conflict resolution
0608	False conflict alert
0674	Flightplan is incorrectly revised by pilot

6. Develop risk assessment model

The next step is to develop a mathematical model of the XFF operation, restricted to the situation of the two opposite direction parallel lanes, which covers as many hazards as possible. For this model, the Dynamically Coloured Petri Net (DCPN) formalism [18], [19] is used, which is a particular Petri net extension.

6.1 Petri net formalism

An (Ordinary) Petri net is a graph of places (representing possible conditions or modes), transitions (which model switches between these modes), and arrows (which connect the places with the transitions). Tokens residing in the places denote which modes are current. If all places by which a transition is connected through an incoming arrow (these places are its input places) are current, then the transition is *enabled*, and fires, i.e. it removes the tokens from its input places, and produces tokens for its output places, thus modelling a mode switch. An uncomplicated example would be:

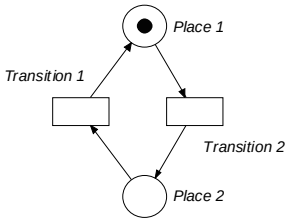

Figure 3: Petri net example. A token resides in Place 1, denoting that that place is the current mode or condition. Transition 2 has a token in its input place, hence is enabled and may fire.

A Dynamically Coloured Petri Net is an extension of Ordinary Petri net in which stochastic differential equations are coupled to places. A token in a place has a colour, assuming a multi-dimensional value, which is the solution of the place-specific stochastic differential equation. A transition which has tokens in each of its input places takes their evolving colours into account: the transition may fire after a particular stochastic colour-dependent delay, or it may fire when the colours of its input tokens have reached a particular value. After firing, the transition produces coloured tokens in its output places.

6.2 Petri net specification

To specify a DCPN for a particular operation, first, local Petri nets (LPNs) are instantiated for each entity (i.e. for each box in Figure 2). Next, the LPNs are connected to each other with additional arrows, places and/or transitions, modelling the interactions and dependencies between the entities. The whole DCPN model building process usually takes several iterations, in which both the LPNs and the interactions are updated. After the final iteration, the DCPN forms a mathematical model of the evolution of the states (e.g. position and velocity) of flows of aircraft as a function of time, influenced by the behaviour (both nominal and non-nominal: hazards) of all entities existing in the operation.

For the XFF example considered in this paper the DCPN instantiation is specified in [13]; it is composed of 14 LPNs, and has in total 39 places (if one counts for only one aircraft) coupled by transitions and arrows.

6.3 Example Petri net

Figure 4 presents an example of (the graphical part of) two LPNs for XFF and their interconnections. In this figure, on the left hand side there is the LPN for Pilot-flying, on the right hand side there is the LPN for Short term conflict detection and resolution (STCD&R); for an explanation see below the figure.

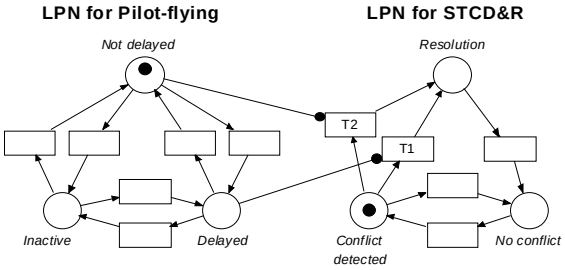

Figure 4: Local Petri nets for entities Pilot-Flying and Short term conflict detection and resolution, and one of their interactions. In this figure, the pilot-flying is in mode *Not delayed*, and the STCD&R is in *Conflict detected*. Transition T2 is enabled and can fire, removing the token from *Conflict detected* (but not from *Not delayed* since the arrow from that place is an enabling arc), and producing a token in place *Resolution*.

The Pilot-flying LPN has three places, which means that three modes are identified for the pilot-flying. There is one *Inactive* mode, which models the situation that this pilot does not act when he should. There are two active modes. In one active mode the pilot has time, is *Not delayed*, and takes proper actions in time. In the other active mode the pilot is *Delayed* and is too preoccupied to act immediately. The *Delayed* mode therefore involves an additional delay in implementing separation conflict recovering actions. The LPN switches between these three modes at random times, with particular switching rates. The colour of the token in this LPN equals the reaction time of the pilot-flying, which is stochastic and dependent on the current mode (e.g. in *Delayed*, this reaction time is larger than in *Not delayed*). Pilot level of skill and training is assumed incorporated in the pilot performance distribution.

The STCD&R LPN also has three places; it models conflict resolution through three modes: In the *No conflict* mode, no separation conflicts are expected in short or medium term. In the *Conflict detected* mode, a conflict has been detected and the automation support proposes a resolution while the resolution has not been acknowledged yet. In the *Resolution* mode the resolution from the automation support has been acknowledged by the pilot-flying and is then implemented automatically. The resolution is continuously up-dated according to the most recent intent information of the intruding aircraft without further pilot acknowledgements. The colour of the token in this LPN contains information necessary for the short term conflict detection and resolution algorithm. In places *No conflict* and *Conflict detected* it contains information like time of closest approach of an intruding aircraft, the identity of the first intruding aircraft, etc. If a separation conflict is expected to occur within the look-ahead

time and the pilot has acknowledged it, place *Resolution* gets a token, with a value equal to a conflict resolution for the aircraft (i.e. a new heading and velocity, until the point where the aircraft can fly in a straight line to the exit point of the sector without causing a conflict). If the conflict has been resolved, place *No conflict* becomes the current one again.

In Figure 4, between these two LPNs two interacting arrows are drawn: One arrow from place *Delayed* to transition T1, and one arrow from place *Not delayed* to transition T2. Both arrows have a small dot at the tip instead of a normal arrow head, denoting that they are *enabling* arcs, i.e. the transition at the tip of the arrow can only fire if there is a token in the place at the beginning of the arrow, but it will not consume this token when it fires. This interaction models that STCD&R can only switch from *Conflict detection* to mode *Resolution* if the Pilot-flying is active, i.e. either *Delayed* or *Not delayed*. As long as the Pilot-flying is in mode *Inactive*, a short term conflict, even if detected by the automatic detection system, is not acknowledged by the pilot, and will therefore not be resolved.

Note that in [13], the descriptions for the LPNs of Figure 4 also include rates or rules for the transitions on when and what to fire, and precise descriptions on how the token colours change through time. Moreover, for simplicity of the figure, there are many more interactions with other local Petri nets that are not drawn.

7. Assess collision risk for model

7.1 Accident risk assessment method

The accident risk assessment makes use of an expression for collision risk [20] which includes as baseline the ICAO-adopted model of Reich [21] for risk of collisions between aircraft. The expression writes collision risk $\Re_{[0,T]}$ within some time interval $[0,T]$, as a function of the incrossing rate $\varphi^{ij}(t)$ of the relative position of two aircraft i and j into some collision area:

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

This incrossing rate might be evaluated using Monte Carlo simulations of the DCPN instantiation. However, since collisions occur very infrequently, they are not counted very often, and direct Monte Carlo simulations may not produce significant results. For this reason, collision risk is decomposed into sums of risk contributions of specifically defined events in time, as in the following equation [22]:

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

where $\varphi^{ij}(t \mid \kappa_{\tau^{ij}} = \kappa)$ is the incrossing rate, conditional on event $\kappa_{\tau^{ij}}$ of type κ at moment τ^{ij}, and $\Pr\{\kappa_{\tau^{ij}} = \kappa\}$ is the probability that event type κ occurs prior to any of the other defined events. If the events are chosen well, each of the individual factors in this expression can be evaluated through dedicated Monte Carlo simulations on the DCPN model.

7.2 Accident risk assessment for XFF

For XFF, for each pair (i,j) of aircraft that meet each other on the opposite direction lanes, 64 event types were identified (i.e. the sum over κ in the equation above has 64 terms); each is composed as follows: For aircraft i there exists a triple (Navigation loop^i, Tactical loop^i, Strategic loop^i) and for aircraft j there exists a triple (Navigation loop^j, Tactical loop^j, Strategic loop^j). Each of the terms in both triples can have values in {Nominal, Non-nominal}. The combination of the two triples yields $2^3 \times 2^3 = 64$ values.

Some explanations of Tactical loop, Nominal, etc, are given in Table 2.

Table 2: Some terms briefly explained

Term	Explanation
Nominal	Behaviour corresponding with the planned ordinary.
Non-nominal	Behaviour corresponding with a deviation from the planned ordinary, e.g. a system failure, a mistake, confusion, a delay.
Navigation loop	Set of LPNs that determine to which extent the aircraft adheres to the ATFM agreed plan. Non-nominal Navigation loop conditions (possibly causing severe deviations from lane) occur e.g. if the pilot accidentally disconnects autopilot, or if the flightplan contains an error, or if the navigation system is not properly working
Tactical loop	Set of LPNs that determine whether the aircraft is able to perform a timely short term evasive manouevre in case of an expected separation conflict. Non-nominal Tactical loop conditions are caused by e.g. pilot being distracted or ADS-B systems not working, any time between time when aircraft meets another on the opposite direction lane and 2 minutes before that.
Strategic loop	Set of LPNs that determine whether the pilots are able to adjust their flightplan to prevent a medium term conflict. Non-nominal Strategic loop conditions are caused by e.g. pilot under-estimates danger of conflict, or ADS-B systems not working, any time between 5 and 2 min before time

	when aircraft meets another on the opposite direction lane

7.3 Accident risk results

By making use of dedicated Monte Carlo simulations on the DCPN instantiation for the XFF example, the factors $\varphi^{ij}(t \mid \kappa_{\tau^{ij}} = \kappa)$ and $\Pr\{\kappa_{\tau^{ij}} = \kappa\}$ in the equation for $\Re_{[0,T]}$ above are assessed for all event types κ, and are combined to obtain accident risk as a function of the spacing parameter *S*. This is the connected curve in Figure 5, which is from [13]. The horizontal axis shows the spacing *S*, the vertical axis shows the number of aircraft accidents per aircraft flight hour that can be expected for this spacing.

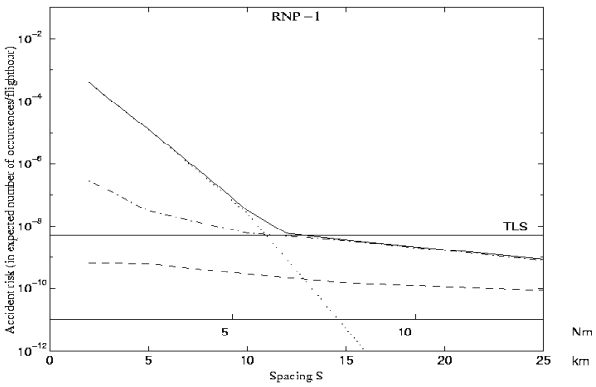

Figure 5: Risk-spacing curve for XFF-DCPN model (—), which is a sum of three curves; '...' denotes contribution to risk from encountering aircraft that are both in Nominal Navigation loop mode; '-·--' denotes contribution to risk from encountering aircraft of which one is in Nominal Navigation loop mode and one is in Non-nominal Navigation loop mode; '---' denotes contribution to risk from encountering aircraft that are both in Non-nominal Navigation loop mode. The horizontal line is a currently applicable Target Level of Safety (TLS) (ICAO) [23].

The risk-spacing curve for the XFF-DCPN model intersects the TLS at *S* = 7 Nm, which would indicate that based on the DCPN model instantiated for XFF operations restricted to a fixed route structure, a distance of *S* = 7 Nm between the parallel lanes is safe.

In Figure 5, the risk-spacing curve is decomposed into a sum of three curves (each curve is based on clusters of event types κ):

- '...' denotes contribution to risk from encountering aircraft that are both in nominal Navigation loop mode (see Table 2);
- '-·--' denotes contribution to risk from encountering aircraft of which one is in nominal Navigation loop mode and one is in non-nominal Navigation loop mode;
- '---' denotes contribution to risk from encountering aircraft that are both in non-nominal Navigation loop mode

It appears that for *S* smaller than 7 Nm, the contribution from encountering aircraft that are both in nominal Navigation loop mode (curve '...') is dominant. For *S* greater than 7 Nm, the contribution from encountering aircraft of which one is in nominal Navigation loop mode and the other is in non-nominal Navigation loop mode (curve '-·--') is dominant. These two contributing factors lead to two curves with different slope. Their sum creates a curve which has a bend.

Further analysis yields that if *S'* (separation minimum) and *S* (spacing) are jointly optimised, the following results are obtained: safe *S'* = 5 Nm, safe *S* = 7 Nm. Moreover, sensitivity analysis shows that for the XFF-DCPN model, accident risk is more sensitive to spacing *S* than to separation minimum *S'*.

8. Bias and uncertainty assessment

So far, we took a formal modelling approach towards the accident risk assessment. This means that accident risk is assessed for the instantiated model of the XFF example. One thing is sure, for operations as complex as the XFF example considered, a model will always differ from reality, and thus model validation cannot be a matter of showing that the model equals reality. The validation problem rather is how to verify that the model 'matches' reality sufficiently well, with respect to the intended use of the model. An absolute 'match' is neither feasible nor necessary. Thus, validation addresses the questions:

- how much differs the instantiated model from reality, and
- how large is the effect of these deviations on the outcomes of the assessment?

Hence, it is necessary to bring the model assumptions made to the foreground and subsequently perform an analysis of their effects on accident risk.

8.1 Model assumptions

Four types of model assumptions are identified in [12] that influence these effects:

- Numerical approximation assumptions;
- Parameter values;
- Model structure assumptions;
- Assumptions due to Non-coverage of hazards.

The effect of each model assumption on accident risk can be of two kinds:

- Bias; due to the adoption of the formal model assumption, the DCPN model-based accident

risk is systematically higher or lower than expected for the real operation.

- Uncertainty; there exists uncertainty in the DCPN model-based accident risk, for example due to uncertainty in the value of some parameter.

8.2 Evaluation of model assumptions

In [14], the bias and uncertainty of each individual assumption has been assessed For the XFF-DCPN model, this covered 122 assumptions:

- 7 assumptions due to numerical approximation have been identified and assessed by an expert of both the DCPN model and its numerical implementation. See Table 3 for two examples.

Table 3: Example numerical approximation assumptions

Id	Assumption	Assessment
nm03	The probability density function of the lateral position of the aircraft is approximated by a sum of Gaussians	Neutral effect
nm04	If the planning loop is non-nominal some time during the planning loop interval, it is considered non-nominal for the complete interval	Negligible pessimistic bias

- 70 assumptions due to selection of DCPN model parameter values have been identified by scanning the DCPN model description as documented in [13], and have been verified by an expert of the numerical implementation of the DCPN model. The bias and uncertainty of these values have been assessed by using statistical data, and by using input from operational experts. The risk sensitivity of these values has been assessed through expert knowledge of the DCPN model and software, and through (partial) accident risk evaluations of the DCPN model. See Table 4 for some examples.

Table 4: Example parameter value assumptions

Sym-bol	Parameter explanation	Value	Assess-ment
$\bar{v}_G$	Average ground speed	250 m/s	Small uncertainty
$v_{\perp}^{\max}$	Maximal rate of climb/ descent	10 m/s	Negligible uncertainty
μ_6^{PF}	Mean duration for Pilot-Flying to perform task when in *Not delayed* mode,	5 s	Minor uncertainty
N_{flow}	The number of aircraft that enters each lane per hour	3.6	Minor uncertainty

- 23 assumptions due to model structure of the DCPN model have been identified and assessed by stochastic experts of the DCPN model. See Table 5 for some examples.

Table 5: Example model structure assumptions

Id	Assumption	Assessment
md01	Aircraft flight plan switches between *Nominal* and *Non-nominal* independent of other local Petri nets	Minor optimistic bias
md06	Stochastic effects due to weather are implicitly incorporated in aircraft evolution model	Negligible optimistic bias
md22	Conflicts are solved sequentially and first in first out.	Negligible pessimistic bias

- 22 assumptions due to non-coverage of hazards have been identified and assessed as follows: Each of the hazards identified for XFF has been analysed by experts of the DCPN model on coverage by the DCPN model. If a hazard appeared not to be covered, an assumption was formulated to explain this. The resulting list of assumptions has been assessed by operational experts. See Table 6 for some examples.

Table 6: Example non-coverage of hazards assumptions

Id	Assumption	Assessment
hc06	Pilot does not disconnect the autopilot deliberately	Negligible optimistic bias
hc16	No conflicts with non-existing aircraft are detected	Zero effect
hc18	For all aircraft, ADS-B works according to specs	Significant optimistic bias

Since the assessments of these assumptions often are subjective, the outcome depends on the availability of capable experts of the model, the accident risk assessment and the operational concepts considered, on the exhaustiveness of the hazard identification, and on the availability of reliable statistical data.

8.3 Combining bias and uncertainty results

Next, all results are combined, following [12], to obtain a model bias compensation factor and 95% credibility interval for risk of the actual operation.

The bias and uncertainty assessment results obtained for realistic XFF operations are given in

Figure 6. These results are based on the XFF-DCPN model results, corrected for the effects of all model assumptions adopted. For comparison, the figure shows the XFF-DCPN model-based risk-spacing curve together with is decomposition as a sum of

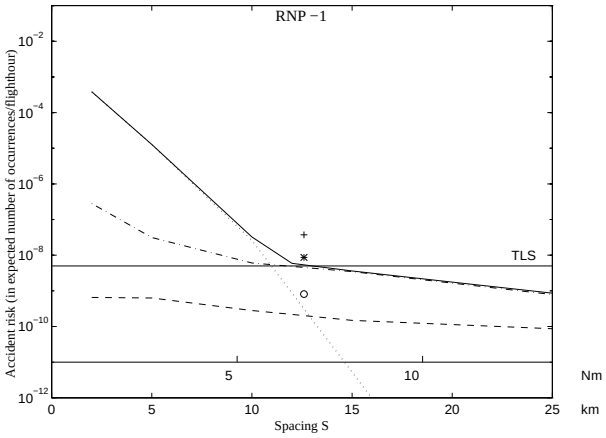

Figure 6: The connected curve is the XFF-DCPN-based risk-spacing curve, decomposed as a sum of three contributions as in Figure 5. The * denotes accident risk for realistic XFF operations, which are obtained by correcting DCPN model-based accident risk for the effects of the four types of model assumptions. The 95% credibility interval for XFF is given by o and +.

Notice that the assessments of the assumptions apply to changes of the risk-spacing curve for the XFF-DCPN model at one value for *S*: at the point where the curve intersects the target level of safety. Also note that some of these assumptions will have an effect on the nominal × nominal curve, others will have an effect on the nominal × non-nominal curve, etc., or even on more than one curve. From this, it is easily seen that the assessments of these assumptions do not necessarily hold for all values of *S*. However, if we assume that they do hold for values of *S* nearby this intersection point, then the expected risk-spacing curve for realistic XFF operations intersects the TLS at S = 9.0 Nm. The assessed 95% credibility interval for realistic XFF accident risk would then intersect the TLS at S = 5.4 Nm and at S = 14.4 Nm.

9. Feedback to airborne separation assurance concept development

The method and results described in Sections 5 through 8 can be used to obtain feedback, both on the on the operation assessed and on the model developed. The first mainly comes from the accident risk versus spacing curves, the latter mainly comes from the bias and uncertainty assessment:

9.1 Feedback on the operation

Based on the risk assessment results obtained, it is possible to identify for some operational aspects how they influence safe *S* values for XFF operations restricted to a fixed route structure:

- A lower flow of traffic between airports A and B in the model is expected to lead to a marginal improvement of the safe *S* value only. The reason is that although accident risk will go down, the quite steep slope of the nominal curve in Figure 6 will prevent the safe *S* value from going down significantly.
- A higher flow of traffic between airports A and B in the model is expected to lead to a significant increase of the safe *S* value. The reason is that accident risk will go up, and the quite shallow slope of the non-nominal curve in Figure 6 will lead to significant increase of the safe *S* value.
- Without the broadcast of intent information by all aircraft it is expected that the safe *S* value increases significantly. The reason is that if pilots are not able to make medium term flight plans that are conflict free then all conflicts have to be resolved on short term; this was studied in [17].
- Leaving out FPCM automation is expected to lead to a significant increase of the safe *S* value. The reason is that in such case the nominal × non-nominal curve is expected to shift to significantly higher risk values.
- Tightening required navigation performance, e.g., from RNP1 to RNP0.3, is expected to lead to a marginal decrease of safe *S* value only. The reason is that the non-nominal contribution curves will hardly change. In Figure 6 this prevents the safe *S* value from going down significantly.
- Relaxing required navigation performance, e.g., from RNP1 to RNP5, is expected to lead to a significant increase of the safe *S* value. The reason is that the steep part of the curve in Figure 6 will get a much shallower slope.
- Sensitivity analysis shows that the accident risk is significantly less sensitive to changes in the value of the separation minimum *S'* than to changes in the spacing value *S*.

At all times, one should be aware that the above findings have been obtained within the context of the hypothetical XFF operational concept considered. Nevertheless the findings obtained give a lot of valuable and original insight both into key issues of airborne separation assurance design and in safe spacing and separation criteria assessment for advanced ATM.

9.2 Feedback on the risk assessment

The bias and uncertainty assessment in [14] showed that the main factors contributing to bias and uncertainty in the model assessed risk values are:

- Response times of the pilots to CD&R and FPCM messages when they are busy with other tasks.
- Aircraft that do not have a properly working ADS-B on board.
- Short term CD&R also proposing vertical escape manoeuvres.

These factors are potential candidates to be further studied on safety and when better understood they may be used to improve the XFF-DCPN model, and subsequently be incorporated in the risk assessment in order to reduce bias and uncertainty.

10. Concluding remarks

10.1 Accident risk results

In this paper, a hypothetical airborne separation assurance operational concept has been evaluated on safe spacing and separation criteria. This is done by assessment of both the model based risk and the bias and uncertainty that is caused by differences between the model and reality. In particular, due to the decomposition of the total risk curve into different contributing terms, the results deliver valuable feedback to airborne separation assurance design. In fact, some of these feedback results have already been obtained in [13]. However, it is due to the added bias and uncertainty assessment of [14] that we reached a level of confidence necessary for publishing the results. We also believe there is room for valuable extensions in the bias and uncertainty assessment performed: a bias and uncertainty assessment should be done for all values of *S*, and for each of the three risk contributing terms separately.

10.2 Beyond operation considered

It should be clear that the results of this study are not intended to provide a definitive answer to questions like "Is Airborne Separation Assurance safer and more capacitive than conventional ATM?". In order to answer such questions, many important aspects remain to be studied, such as:

- Pilot-not-flying monitoring the traffic; is this manageable for the pilot?
- Aircraft flying outside the known route structures; what is the impact?
- The Airborne Separation Assurance operational concept considered in this study may differ from other Airborne Separation Assurance operational concepts under development.
- Many encounter scenarios have not been assessed.
- The XFF scenario considered puts high requirements on conflict trajectory planning and negotiation even between aircraft that are more than 5 minutes apart. These requirements are sufficient but may not be necessary.
- Contributions from Ground ATM are not considered in this study.

Reasonably, these aspects have to be understood before one can draw final conclusions on safety and capacity comparison between conventional ATM and free flight. This asks for additional risk assessments and these are the subject of follow-up study.

10.3 Further developments

The TOPAZ risk assessment methodology has been applied to many other operations and encounter scenarios, including several operations that were developed for short-term introduction. These applications showed that the method works during both early and late life cycle phases of rather complex operations and can provide valuable feedback and insight into the safety/capacity aspects of the operation analysed.

For most stages of the TOPAZ risk assessment methodology, further developments are ongoing in collaboration with other researchers [24], e.g. on the following topics:

- During the instantiation of a mathematical model the graphs of the Local Petri nets and their interactions may become very cluttered and unreadable for complex applications with many interacting entities.
- The decomposition of accident risk assessment into conditional Monte Carlo simulations currently is application-specific. Significant improvements on this are under development by exploring sequential Monte Carlo simulation techniques.
- Regarding bias and uncertainty assessment, further research and developments focus on improving how to handle model structure assumptions, operation concept assumptions and non-coverage of hazards assumptions.

Acknowledgement: The authors would like to thank an anonymous reviewer for helpful suggestions in improving the paper.

11. References

[1] Embrechts, P., Kluppelberg, C., Mikosh, T., Modeling extremal events for insurance and finance, Springer, 1997.

[2] Smidts, C., De Vooght, J., Labeau, P.E., Dynamic reliability: future directions. In: Int Workshop Series on Advanced Topics in Reliability and Risk Analysis, University of Maryland, 1998.

[3] Labeau, P.E., Smidts, C., Swaminathan, S., Dynamic reliability: towards an integrated platform for probabilistic risk assessment, Reliability Engineering & Systems Safety, Vol., 68, 2000, pp. 219-254.

[4] ICAO draft airborne separation assistance system (ASAS) circular, Version 3.0, SCRSP, WGW/1, WP/5.0, 2003.

[5] Principles of Operations for the use of ASAS, Action plan 1, FAA/Eurocontrol Co-operative R&D, Version 7.1, 2001.

[6] Safety and ASAS applications, Action plan 1, FAA/Eurocontrol Co-operative R&D, Version 4.1, 2004.

[7] Cohen, S., Hockaday, S. (eds), A concept paper for separation safety modelling, an FAA/ Eurocontrol cooperative effort on air traffic modelling for separation standards, FAA and Eurocontrol, Brussels, May 1998.

[8] Geisinger, K.E., Airspace Conflict Equations, Transportation Science, Operations Research Society of America, Vol.19, No. 2, May 1985.

[9] ICAO, Review of the general concept of separation panel, 6th meeting (28 November-15 December 1988), Montreal, Doc 9536, RGCSP/6, Volume 1, December 1988.

[10] Sheperd, R., Cassell, R., Thava, R., Lee, D., A reduced aircraft separation risk assessment model, Proc. AIAA Guidance, Navigation and Control Conf., New Orleans, August 1997.

[11] Blom, H.A.P., Bakker, G.J., Blanker, P.J.G., Daams, J., Everdij, M.H.C., Klompstra, M.B., Accident risk assessment for advanced ATM. In: Air Transportation Systems Engineering, G.L. Donohue and A.G. Zellweger (Eds.), Progress in Astronautics and Aeronautics, Vol. 193, AIAA, Reston, Virginia, 2001, pp. 463-480.

[12] Everdij, M.H.C., Blom, H.A.P., Bias and uncertainty in accident risk assessment, Report TR-2002-137, National Aerospace Laboratory NLR, Amsterdam, 2002.

[13] Daams, J., Bakker, G.J., Blom, H.A.P., Safety evaluation of encounters between free-flight equipped aircraft in a dual route structure, Report TR-99577, National Aerospace Laboratory NLR, Amsterdam, 1999.

[14] Everdij, M.H.C., Bakker, G.J., Blom, H.A.P., Bias and uncertainty in accident risk assessment of the Extended Free Flight operational concept, Report TR-2002-691, National Aerospace Laboratory NLR, Amsterdam, 2002.

[15] Hoekstra, J.M., Ruigrok, R.C.J., Van Gent, R.N.H.W., Conceptual design of free flight cruise with airborne separation assurance, Report TP 98252, National Aerospace Laboratory NLR, Amsterdam, 1997.

[16] Free Flight research issues and literature search, Under NASA contract NAS2-98005, J. Krozel, 2000.

[17] Daams, J., Bakker, G.J., Blom, H.A.P., Safety evaluation of an initial free flight scenario with TOPAZ, Report TR-98098, National Aerospace Laboratory NLR, Amsterdam, 1998.

[18] Everdij, M.H.C., Blom, H.A.P., Petri-nets and hybrid-state Markov processes in a power-hierarchy of dependability models, Proc. IFAC Conf. Analysis and Design of Hybrid Systems 16-18 June 2003, Saint-Malo, Brittany, France.

[19] Everdij, M.H.C., Blom, H.A.P., Piecewise Deterministic Markov Processes represented by Dynamically Coloured Petri Nets, To appear in Stochastics and Stochastics Reports, February 2005.

[20] Bakker, G.J., Blom, H.A.P., Air Traffic Collision risk modelling. In: Proc. 32nd IEEE Conference on Decision and Control, 1993, pp. 1464-1469.

[21] Reich, P.G., Analysis of long range air traffic systems: Separation standards—I, II, and III . Journal of the Institute of Navigation 19: 88- 96, 169-176, 331-338, 1966.

[22] Blom, H.A.P., Bakker, G.J., Everdij, M.H.C., Van der Park, M.N.J., Collision risk modeling of air traffic, Proc. IFAC European Control Conference 2003, Cambridge, UK, September, 2003.

[23] ICAO Annex 11 - Air traffic services, 12th edition, incorporating amendments 1-38, Green pages, attachment B, paragraph 3.2.1, July 1998.

[24] HYBRIDGE project, http://www.nlr.nl/public/hosted-sites/hybridge