Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2002-690

Human cognition performance model to evaluate safe spacing in air traffic

H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij, M.N.J. van der Park

This report is based on a paper published in Human Factors and Aerospace Safety, Vol. 3, 2003, pp. 59-82.

Division:	Air Transport
Issued:	November 2003
Classification of title:	Unclassified

Abstract

This paper develops a mathematical model for cognitive performance of a tactical air traffic controller in an en-route air traffic context. The aim of this model-based approach is to enable the evaluation of both accident risk and aspects like cognitive workload and effectiveness in managing air traffic safely. Use is made of human error modelling, Hollnagel's cognitive mode model and Wicken's Multiple Resources model. The paper describes how these psychological sub-models are combined into a single model of controller cognitive performance, and how the interaction of these human sub-models with the technical sub-systems is brought into account. The approach is applied to evaluate safe spacing for a conventional air traffic control example. The evaluation includes a bias and uncertainty assessment, and a safety criticality analysis.

Contents

(28 pages in total)

1 Introduction

1.1 Safety based air traffic management design

Over decades, the aviation industry has been able to compensate the increase in traffic with a decrease in accident risk per flight hour. In view of the rapid growth of air traffic and the technological and organisational complexity of it, this has been a major accomplishment. Unfortunately, the point has been reached where it is unclear how to continue such compensation. The reason is that in the past the decrease in risk per flight hour has come in large part from technology driven improvements of safety. The effect of this technology-driven approach is shown through the accident statistics; they reveal that the relative share of human related causes is some eighty percent. This means that the historical air traffic safety compensation process can be continued if one learns to understand how the human and procedure related accident risk could be mitigated. This should be accomplished by learning the principles behind human related accident risk in aviation.

If we try to understand these principles on the basis of an evaluation of incidents and accidents alone, then several difficulties arise. The number of incidents and accidents is limited, while the situations that caused them are quite complex (e.g. Rodgers et al., 1998). Moreover a retrospective learning approach does not work for advanced air traffic management concepts. By now there is a broad consensus that appropriate prospective safety models are needed to assess accident risk in relation to separation criteria and near-misses (Cohen and Hockayday, 1998) with the aim to optimise advanced air traffic operations (Haraldsdottir et al., 2001; Odoni et al., 1997; Wickens et al., 1998).

1.2 Air traffic safety modelling

In air traffic there are various human operators: a crew in each aircraft and ground sector air traffic controllers, who all have an active role in maintaining air traffic safety. In comparison with other safety critical operations the safety of air traffic is by its very nature highly distributed. This is depicted in Figure 1. Because of the distributed control nature of air traffic, established techniques fall short in performing accident risk assessment. Blom et al. (2001a) addressed this problem by developing a stochastic analysis based methodology that takes an integral approach towards accident risk assessment for air traffic. It has also been studied how this approach effectively supports safety management and the building of modern Safety Cases for advanced operations in air traffic (Blom et al., 1999).

1.3 Human performance modelling

A crucial issue in air traffic safety evaluation is how the human factor is incorporated into the risk model. Hence there is a clear need for a modelling approach to assess and understand accident risk in relation to the performance of the human operators involved. This means that appropriate human performance models are required that describe human responsibility and cognitive principles up to the level of accident risk. This paper aims to present the developments of such a human cognition performance model for a tactical controller within the context of conventional en-route Air Traffic Control (ATC). This development is based on the following three complementary psychological models:

- Multiple Resources Model (Wickens, 1992)
- Human Error Modelling (e.g. Kirwan, 1994)
- Contextual Control Mode Model (Hollnagel, 1993)

The first two of these three psychological models are well known in aviation (e.g. AGARD, 1998; Corker, 2000; Isaac and Ruitenberg, 1999; Kilner et al., 1997). The development of Hollnagel's control mode model for controller cognitive performance and air traffic safety is novel.

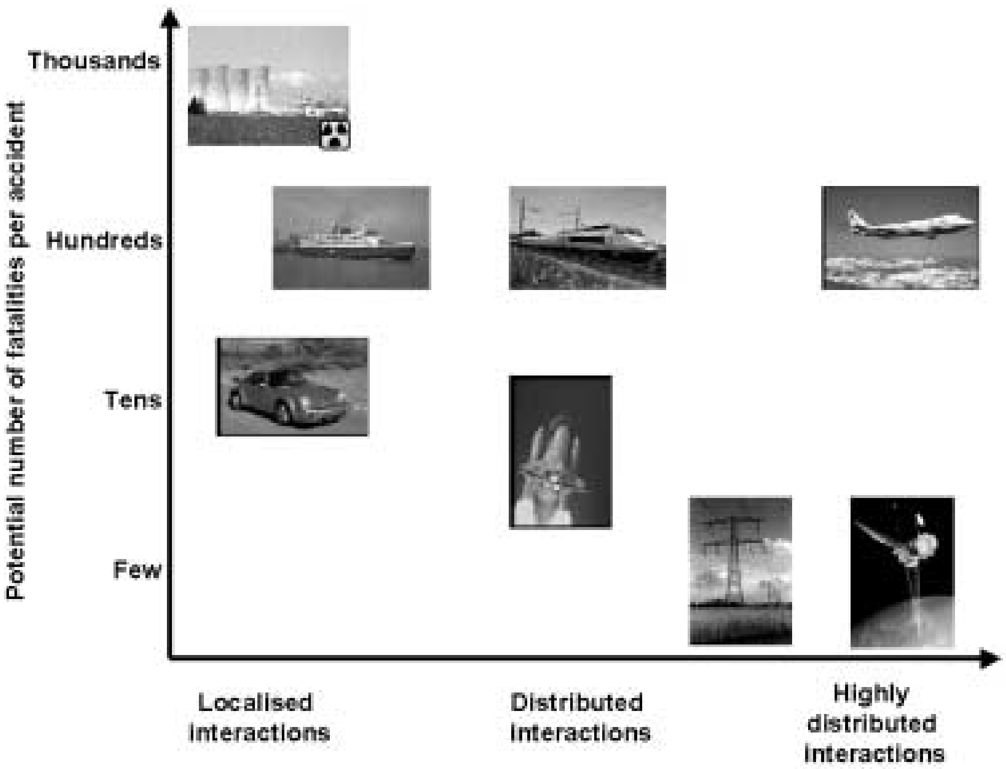

Figure 1 Potential fatalities and level of distributed interactions of air traffic and other safety critical activities.

At present, the view on human reliability has shifted from a context-free error centred approach, in which unreliability is modelled as failures of human information processing, towards a contextual perspective in which human actions are the product of human internal states, strategies and the environment (Amalberti and Wioland, 1997; Hollnagel, 1993; Bainbridge, 1993). From this viewpoint, safety critical human actions should be modelled in their relation to the other activities of the operator and the environment. Thus for a proper description of human reliability it is necessary to include the cognitive processes that underlie the operator actions. As a result, one obtains a comprehensive model of the operator performing his job.

1.4 Organisation of this paper

This paper is organised as follows. The following section provides the background of psychological models used to model an air traffic controller. In the next section this mathematical model is integrated with the other air traffic systems. This integrated model is then used to assess an operational concept on controller performance and accident risk. Next, a bias and uncertainty assessment is performed. In the final section we discuss the results obtained.

2 Psychological modelling

The aim of this section is to show how the complementary psychological models are used to develop a mathematical model of a tactical controller performing his job at a high (cognitive) level in an en-route ATC environment.

2.1 Decomposition of the Controller's task

The controller's task is decomposed into several subtasks. This decomposition has been carried out along two dimensions: first a *generic dimension*, where the task is decomposed into cognitive activities at a general level which is independent from the scenario and operational concept. Secondly, the task is decomposed according to a *scenario/concept specific dimension*, where the controller task is described at the level of operational functions in the scenario.

A task decomposition along the generic dimension originates in the work of Jackson (1989). Subsequently, Buck et al. (1996) merged this with other task analyses (Ammerman et al., 1987; Cox, 1994; EATCHIP, 1996; Endsley and Rodgers, 1994). The following subtasks resulted:

1. *Sensing* Gathering all information which is needed to get an overview over the air traffic situation.
2. *Integration* Connecting the gathered information thus forming a more global air traffic picture.
3. *Prediction* Using the global picture to anticipate future situations and events.
4. *Complementary communication* Passing the information to aircraft in order to improve the pilots understanding of the situation.

5. *ATC problem solving and planning* Using the understanding gained from the more global perspective to plan and prioritise aircraft actions.
6. *Executive action* Communicating information and priorities as instructions to the aircraft in the system.
7. *Rule monitoring* Ensuring that the active components of the system behave in accordance with the 'rules'; monitoring and taking corrective actions for exceptions.
8. *Co-ordination* Co-ordinating laterally with other parts of the ATC organisation).
9. *Overall performance* Ensuring that the objectives of the operation are achieved, and that the infrastructure functions correctly.
10. *Maintenance and monitoring of non-human part* Ensuring that all systems supporting the controller work correctly.

Secondly, following Daams et al. (2000), subtasks are also defined along the en-route ATC specific dimensions, where attention is focused on safety critical actions in the definition of the subtasks. This leads to the identification of three en-route context specific tasks:

A. Anticipate for aircraft deviating from intentions.
B. React to Automation alerts.
C. Perform other control activities.

Next, we identified the task overlap *across* the dimensions in Table 1. This leads to 19 combinations across the dimensions, and thus a decomposition into 19 combined controller subtasks.

Table 1 Task overlap across the generic cognitive activities and the en-route ATC specific tasks

	A **Anticipate**	**B** **Alerts**	**C** **Others**
1. Sensing	X		X
2. Integration	X		X
3. Prediction	X		X
4. Complementary comm.			X
5. Problem solving /planning	X	X	X
6. Executive action	X	X	X
7. Rule monitoring	X	X	X
8. Co-ordination			X
9. Overall performance			X
10. Maintenance			X

2.2 Hollnagel's control modes

Hollnagel (1993) developed an approach that is complementary to task modelling. It focuses on different control modes of the human operator's cognition, which reflect different control strategies in operator behaviour.
The specific four control modes that are described by Hollnagel (1993) characterise in more detail regions of the continuum of control and can be specified as follows:

Scrambled Scrambled control denotes the case where the choice of the next action is completely unpredictable or random. The scrambled control mode includes the extreme situation of zero control.

Opportunistic Opportunistic control corresponds to the case when the next action is chosen from the current context alone, and mainly based on salient features rather than on more durable intentions or goals. It is opportunistic in the sense that the operator takes a chance, not because he is deliberately exploring an alternative, but because there is no time or possibility to do anything better.

Tactical Tactical control is characteristic for situations where the operator's performance is based on some kind of planning. Hence, the operator more or less follows a known procedure or rule. The planning is limited of scope and/or limited of range, and the needs taken into account may sometimes be ad hoc.

Strategic Strategic control means that the operator is considering the global context, i.e. using a wider event-horizon and looking ahead at higher level goals: either those which have been suspended and have to be resumed or those which, according to experience and expectations, may appear in the near future. This mode should provide a more efficient and robust performance.

To model the influence of the context on performance, we follow Daams et al. (2000) and incorporate two control modes: tactical control and opportunistic control. Table 2 describes the characteristic influence of these control modes on the performance of the category A subtasks. These characterizations appeared to be easily available from air traffic controllers. For the category B subtasks a similar characterization applies. For category C subtasks it suffices to describe differences in tactical and opportunistic control mode only at a general level. Table 2 illustrates that the quality of performing a subtask may vary significantly with the cognitive control mode of the controller.

Table 2 Control mode characteristics of subtasks related to anticipation

A1	**Sensing**
	Tactical: Whenever possible the controller scans his display to detect possible deviations from ATC intentions. The controller partitions the display into regions of interest and assesses these regions in a particular order. If scanning is interrupted at some time instant, the controller will resume scanning starting at the region that he was scanning when the interruption took place. Further information may also be obtained through R/T communication. *Opportunistic*: Whenever possible the controller scans his display to detect possible deviations. The controller scans in a random fashion.
A2	**Integration**
	Tactical: The controller systematically integrates the information derived from scanning to improve his mental picture of the traffic situation. When some relevant information is not available, the controller may return to sensing to actively seek information to improve his assessment of the situation. *Opportunistic*: The controller integrates the randomly obtained information. An incomplete or even distorted mental picture may develop.
A3	**Prediction**
	Tactical: The controller extrapolates his mental picture to the future traffic situation. On the basis of the assessment of the situation, the controller decides whether a problem may occur in the mid-term future. *Opportunistic*: The assessment of the future situation is restricted to a short time horizon and is based on incomplete information. It is assessed whether a problem may be expected in the short-term future.
A5	**Problem solving/planning**
	Tactical: On the basis of the assessment of the (future) situation, the controller decides a resolution to the expected problem. In principle, the resolution involves replanning the aircraft trajectories in an optimal fashion with respect to safety, efficiency. *Opportunistic*: The resolution is aimed at solving the imminent problem only.
A6	**Executive action**
	Tactical: The controller gives a series of R/T instructions to the aircraft involved. He verifies whether the pilot(s) readback these instructions correctly. *Opportunistic*: The verification of correct readback may be omitted.
A7	**Rule monitoring**
	Tactical: After the R/T communication the controller verifies whether the aircraft comply to his clearances. *Opportunistic*: This verification may be omitted or be performed less thoroughly.

2.3 Aggregation of subtasks

Next the 19 subtasks are grouped into a smaller number of clusters. The adopted clusters are given in Table 3. The rationale for this clustering is as follows. Subtasks of category A and B are grouped when they are nominally performed in a sequence (A1-A3), (A5-A7), (B5-B7). Each safety relevant subtask of category C forms its own cluster, while the other category C subtasks are grouped in the cluster Miscellaneous.

Table 3 Clustering of the subtasks

Cluster	Initial subtasks
Monitoring_A	A1-A3
Communication_A	A5-A7
Communication_B	B5-B7
$\text{Complementary Communication}_C$	C4
Communication_C	C6
Co-ordination_C	C8
Miscellaneous_C	C1-C3, C5, C7, C9, C10

Next, based on knowledge of Wickens' Multiple Resources model for controllers, we identified how task scheduling at the level of clusters of subtasks takes place. First, concurrent performance of the initial subtasks has been used to identify the concurrency for the subtask clusters. This is done conservatively using the principle that if one combination of the clustered subtasks cannot be performed concurrently, then the whole cluster of subtasks cannot be performed concurrently. Application of this principle yields concurrency for two clusters only: Miscellaneous and Monitoring. In a similar fashion, Table 4 for the pre-emption between clusters of subtasks has been identified. First this was done for the initial subtasks and was based on knowledge of the Multiple Resources Model for controllers. Subsequently the following pre-emption rule was applied: if any subtask in some cluster X pre-empts all subtasks in some cluster Y, then cluster X pre-empts cluster Y. Otherwise, cluster X does not pre-empt Y.

Table 4 Pre-emption between clusters

	Mon_A	**Com_A**	**Com_B**	**CpC_C**	**Com_C**	**Coor_C**	**Misc_C**
Mon_A		N	N	N	N	N	N
Com_A	Com_A		N	Com_A	Com_A	Com_A	Com_A
Com_B	Com_B	Com_B		Com_B	Com_B	Com_B	Com_B
CpC_C	CpC_C	N	N		N	N	CpC_C
Com_C	Com_C	N	N	Com_C		Com_C	Com_C
Coor_C	Coor_C	N	N	Coor_C	N		Coor_C
Misc_C	N	N	N	N	N	N	

The pre-emption table should be read as follows. Consider subtasks Com_B and Com_A in Table 4. In the column corresponding to Com_A, we see that Com_B pre-empts Com_A. Thus if Com_A is carried out and Com_B is initiated, execution of Com_A will stop and Com_B will be performed first. In terms of a stack of to-be-performed subtasks this scheduling principle can be formulated generically as the following two rules.

Rule 1: An initiated subtask will be placed in the execution stack before the subtasks that it may pre-empt.

Rule 2: If the first two subtasks of the execution stack can be processed concurrently, this will be done (subtask duration will be slightly longer, however).

Following Table 4 the cluster $Miscellaneous_C$ does not pre-empt any other cluster and is pre-empted by all other clusters, except $Monitoring_A$. Furthermore, since $Monitoring_A$ and $Miscellaneous_C$ can be performed concurrently, we conclude that performance of the subtasks in the cluster $Miscellaneous_C$ does not conflict with other subtasks at cluster level. Since the cluster $Miscellaneous_C$ itself does not contain subtasks that are directly relevant for safe separation, we can therefore discard this cluster in the model without compromising conservativeness. Altogether Table 4 implies that the remaining pre-emption rules boil down to a fixed priority list where $Monitoring_A$ has lowest and $Communication_B$ has highest priority. At the level of clustered tasks, the complexity of the scheduling principle is reduced significantly, without compromising conservativeness. In summary, we accomplished a reduction from 19 subtasks to six clusters of subtasks, the concurrent task performance is simplified into single task performance, and pre-emption rules for each combination of subtasks are simplified into a fixed priority list (see table 5).

Table 5 Six main cognitive tasks

Task	**Priority**	**Description**
$Monitoring_A$	6	Visual anticipation and detection of deviations from the controller intention
$Communication_A$	2	Communicate clearance with aircraft that was detected visually to deviate severely from controller intention
$Communication_B$	1	Communicate clearance with aircraft for which an Automation alert was issued
Complementary $communication_C$	5	General complementary communication with pilots
$Communication_C$	3	General communication of executive action (i.e. clearances)
$Co\text{-}ordination_C$	4	General co-ordination with planner controller, controllers of other sectors.

3 Integration with air traffic systems

In this section we illustrate how the controller model developed in the second section is integrated with the other elements of an air traffic example.

3.1 Hypothetical ATC example

We consider an hypothetical ATC example within an en-route sector that consists of two streams of air traffic, flying in opposite direction, at a single flight level. This example has been developed by Eurocontrol with the aim to learn understanding how ATC influences accident risk, and how far the nominal spacing *S* between opposite RNP1 traffic streams can safely be reduced. The specific details of this example are:

- Straight route, with two opposite traffic lanes (Figure 2 shows top view)
- Air traffic controller (ATCo) allowed minimum separation between aircraft is 5 NM and distance between the two traffic lanes is *S*
- ATCo expects aircraft to stay on these lanes
- Traffic flows along each lane at one flight level only, with 3.6 aircraft/hour per lane and 15 aircraft per controller
- All aircraft nominally perform RNP1
- None of the aircraft are TCAS equipped
- No military aircraft.

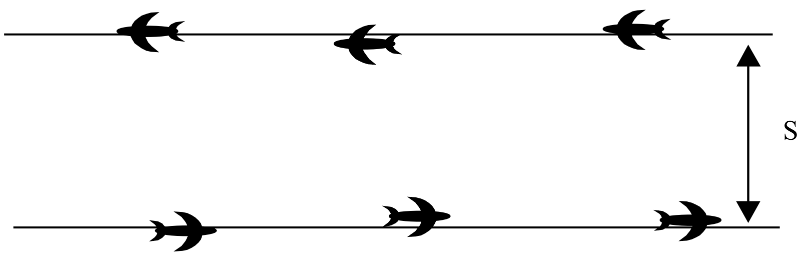

Figure 2 Opposite direction traffic lanes at one flight level

This traffic scenario is considered for a conventional ATC concept of routine monitoring-based control of traffic (Figure 3). There is radar-based surveillance and radio communication, but no automation support tools. Aircraft deviations are identified through routine monitoring by the controller.

3.2 Errors in flightplans and intentions

An important safety issue is that for one single aircraft there may be all kind of differences between the flight's intentions on the ground and in the air, and the controller and pilot awareness of those intentions, i.e.:

- Controller's awareness of the flight's intentions
- Flightplan in the ATC system
- Pilot's awareness of the flight's intentions
- Flightplan used by the FMS

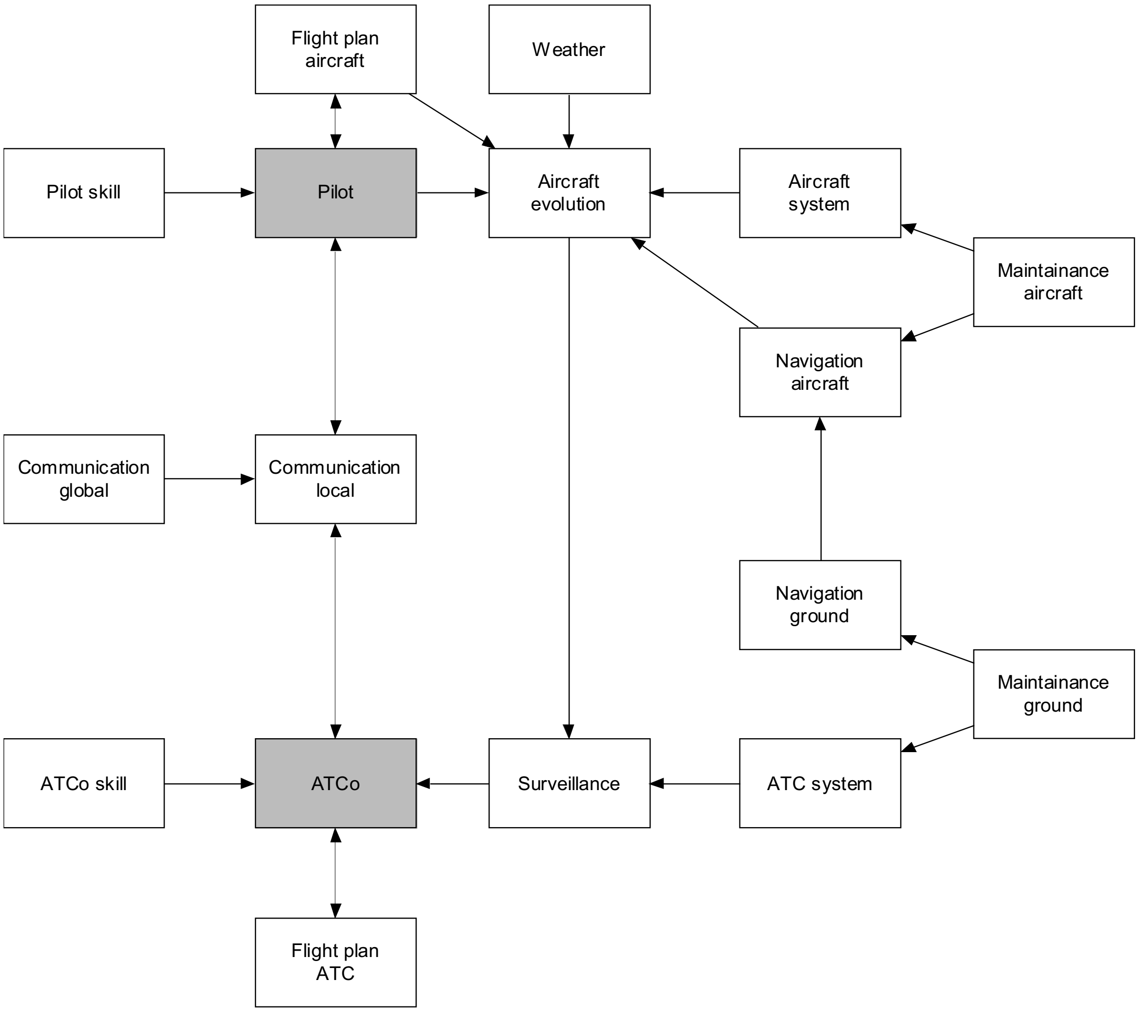

Figure 3 Functions in conventional ATC.

To allow for these differences the following mathematical modelling approach is adopted:

Controller The tactical controller's awareness of the flight's intentions is assumed to be ATC's true reference. The quality of ATC's true reference is in one of the following two discrete modes: i) the true reference provides separation, ii) the true reference does not provide separation. In general the latter mode value may be reached if a controller has made a knowledge-based error.

ATC The quality of the flightplan in the ATC system may be in one of the following two discrete modes: i) agrees with ATC's true reference, ii) differs from ATC's true reference. The latter is due to a controller input error, or an ATC database error.

Pilot The quality of the pilot's awareness of ATC's true reference is in one of the following two discrete modes: i) agrees with ATC's true reference, ii) differs from ATC's true reference. The latter may happen due to a clearance error. There are two types of clearance errors: 1) intended clearance given to wrong aircraft or 2) wrong clearance given to intended aircraft. The cause may be with the controller, or the pilot or both, and may be knowledge-based, rule-based or skill-based.

FMS The quality of the flightplan used in the FMS is in one of the following two discrete modes: i) agrees with ATC's true reference, ii) differs from ATC's true reference. The latter happens if pilot awareness differs from ATC's true reference or is due to a pilot input error or an FMS database error.

In elaborating the above it is assumed that all the controller related errors may occur at random during performance of subtasks A6, B6 or C6, (executive action) where the frequency of occurrence depends on the control mode the controller is in. Furthermore, such errors may be detected and corrected during rule monitoring subtasks A7, B7 or C7, which also depends on the control mode (e.g. Amalberti and Wioland, 1997).

3.3 Petri net model of the ATC example

To integrate in a systematic way the elements of the air traffic en-route concept shown in Figure 3, including the six main controller cognitive tasks identified in the second section, we use a dedicated Dynamically Coloured Petri Net (DCPN) specification formalism. A DCPN is a general formalism to represent a dynamical stochastic system with discrete and continuous-valued states (Everdij and Blom, 2000). For the ATC example considered in this paper the DCPN instantiation is specified in Stroeve et al. (2002).

As a part of the complete DCPN, the Petri Net describing the discrete modes for the controller model is given in Figure 4. In this Petri Net the six main cognitive tasks of Table 5 are represented. For each task, we assume a relative priority ranking, an average duration under the opportunistic and tactical control modes and the percentage of his time that the operator would spend on the task if uninterrupted. The controller performs these tasks one at a time, according to the given priorities. Task scheduling is kept straightforward: high priority tasks are performed first, possibly interrupting a low priority task. Furthermore, Figure 4 shows the two cognitive control modes of the air traffic controller: *Tactical* and *Opportunistic*. The switching between the control modes depends on the subjectively available time (measured as the number of tasks waiting to be performed) and the outcome of previous actions (measured as the number of recent corrective actions, i.e. $Communication_A$ and $Communication_B$). If subjectively the available time is short or if the outcome of previous actions is poor then the controller switches to the *Opportunistic* control mode. Controller erroneous clearances are taken into account as follows: the controller may give a different clearance than intended (e.g. switching heading and speed), or may give the clearance to a different aircraft than intended (call-signs mixed up). These errors are incorporated as random variations in the controller actions. The error types are represented in the place *Clearances*.

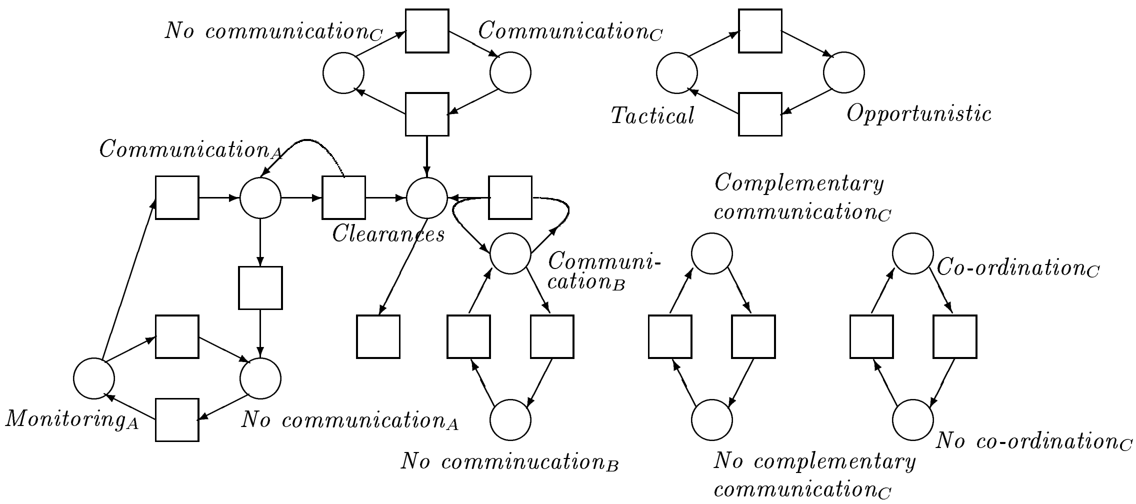

Figure 4 Petri Net of reduced controller model. A circle denotes a discrete state (e.g., the performance of a task) and a square denotes a transition between discrete states.

The switching between the states in the controller model is influenced by several functional entities in air traffic indicated in Figure 3, such as Aircraft evolution, Surveillance, ATC system, R/T local, R/T global, Pilot Performance. Surveillance output (i.e. the estimated aircraft state) is input for the visual detection of severe deviations by the controller. The ATC system must be *Working* for the controller to be able to do his job. The R/T entities and Pilot entity together form the Decision Making loop (DM-loop). If none of the entities in the DM-loop is *Down* or *Inactive* for a given aircraft, then the controller is able to give a clearance to that aircraft. Properly integrated, these entities together represent the air traffic control concept discussed at the beginning of this section. Once having developed this DCPN instantiation, it is possible to both implement and run a Monte Carlo simulation and combine this with stochastic analysis based collision risk evaluation for this model (Blom et al., 2001b).

4 Model based results

Based on the mathematical model we ran Monte Carlo simulations in order to assess controller reaction times, controller cognitive performance and accident risk for the model.

4.1 Controller reaction times

For the controller routine monitoring concept we evaluated the period used to detect severe deviations so that a comparison with available statistical data was possible (George et al., 1973). Comparison, in Figure 5, with the model based results shows that the detection time results of both the original and the reduced controller model agree quite well with the measured data. It should be noticed that George et al. (1973) measured very few detection times beyond 150 seconds were measured. Although these longer detection times have low probability, these times add significantly to the risk, and Figure 5 shows that model based results do extend to these low probability values. We may conclude that both the full and the reduced model curves agree quite well with the statistical data. This clearly contributes to gaining confidence in the model-based approach taken.

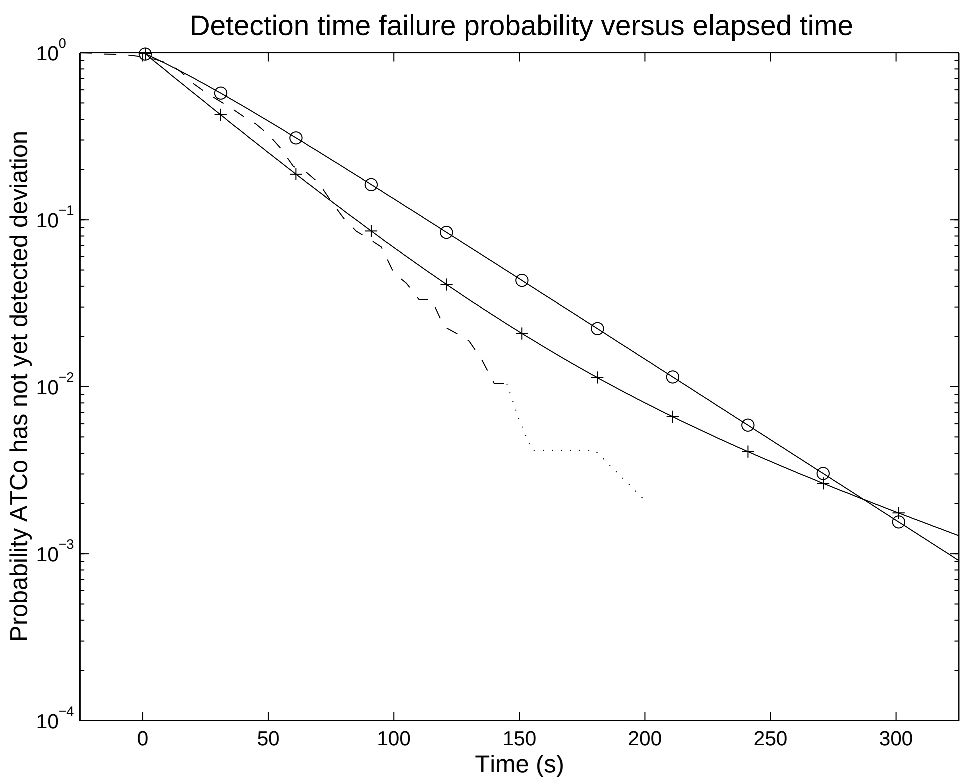

Figure 5 Controller detection time of severe deviations of the full model (line marked '+'), of the reduced model (line marked 'o') and of statistical data (George et al., 1973) (dashed/dotted line, the dotted part representing data based on less than 5 measurements).

From Figure 5 it appears that our reduced model yields only slightly more conservative controller detection time results. Therefore we conclude that for the particular application considered here, incorporation of concurrent task processing into the controller performance model is not necessary for avoiding overly conservative risk estimates. Obviously, incorporation of concurrent processing into human performance models may be essential for other applications such as detailed workload assessment.

4.2 Controller cognitive performance

The proportions of the various controller tasks, following from simulation of the ATC model, are shown in Table 6. In the model the controller is about 35% of the time not involved in any task, about 25% of the time specifying general clearances (Communication_C), about 22% of the time communicating with aircraft crews not involving clearances (Complementary Communication), about 9% of the time coordinating with other controller's, about 8% of the time monitoring the traffic display and about 2% of the time specifying back-to-lane clearances as a result of monitored deviations (Communication_A).

Table 6 Relative task times for the various controller tasks and the relative time spent in the opportunistic cognitive mode. The tasks are ordered from high to low priority.

Task	Time (%)	Opportunistic (%)
Communication_B	0	n.a.
Communication_A	2	3
Communication_C	25	19
Coordination	8	47
Complementary Comm.	22	16
Monitoring_A	8	1
Miscellaneous	35	0

The results show that monitoring and the specification of clearances as a result of monitored deviations is almost always (>96%) done in the tactical control mode. The low contribution of opportunistic control during monitoring is a result of the low task priority given to monitoring in the model. In particular, monitoring is only performed if no other tasks are pending. This results in a low workload, implying that this task is almost always done with a tactical control mode. The small share of opportunistic control during the specification of clearances as a result of monitored deviations (Communication_A) can be explained by the notions that this task directly follows monitoring, which is mostly done under tactical control, and that the task is short lasting.

It follows from Table 7 that the ratio of opportunistic control increases with the task priority for complementary communication and co-ordination, which are performed about 16% and 47% of the time in the opportunistic control mode, respectively. However, for the specification of general clearances (Communication$_C$), which has priority over co-ordination, a decrease in the opportunistic mode share can be observed. This may be explained by the relatively long duration of co-ordination tasks (see Table 7), such that the chances are high that a complementary communication or monitoring task become pending during a co-ordination task, whereas the probability that tasks with a lower priority become pending during the specification of general clearances (Communication$_C$) is more modest.

Table 7 Mean task duration and the mean time the process is pending due to a process with a higher priority. The tasks are ordered from high to low priority.

Task	Mean duration (s)	Mean pending (s)
Communication$_B$	n.a.	n.a.
Communication$_A$	6.4	0
Communication$_C$	13	0.1
Coordination	28	8.3
Complementary. Comm.	14	9.6
Monitoring$_A$	7.1	17

4.3 Accident risk of model

Using dedicated Monte Carlo simulations (Blom et al., 2001b) for the ATC example we assessed accident risk as a function of the spacing parameter *S*. The accident risk results are presented in Figure 6. In Figure 6, the risk-spacing curve is decomposed into a sum of three curves:

- the curve 'Nominal' denotes the risk contribution from encountering aircraft that both evolve along their lanes as expected by the ATCo, while communication and navigation entities are working;
- the curve 'Communication & Navigation Up × Sharp-turn(s)' denotes the risk contribution from encountering aircraft of which at least one makes an ATCo unexpected sharp turn, while communication and navigation entities are working;
- the curve 'Others' denotes the risk contribution from encountering aircraft for all other off-nominal event types.

Figure 6 shows that the first two events types almost completely determine the total risk curve. The total risk curve crosses the ICAO defined TLS (Target Level of Safety) level at $S = 13.5$ NM. This means that a safe spacing value for the model is 13.5 NM. Of course the key question is, what does this mean in reality?

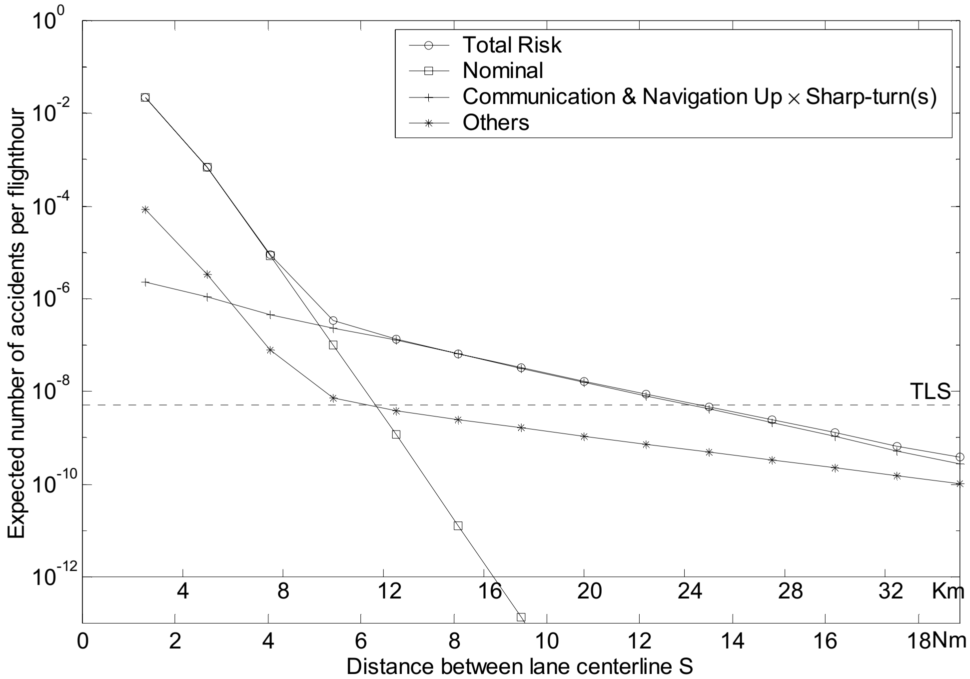

Figure 6 ATC routine monitoring model-based accident risk curve. The horizontal line is the Target Level of Safety (TLS) of (ICAO, 1998). See the main text for an explanation of the curves.

5 Risk model validation

So far we took a formal modelling approach towards the accident risk assessment. This means that for the instantiated model of the ATC example accident risk and controller performance indicators are assessed. One thing is certain, for operations as complex as the ATC example considered, a model will always differ from reality, and thus model validation can not 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 does the instantiated model differ 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 into the foreground and subsequently perform a bias and uncertainty analysis of the model versus reality.

5.1 Bias and uncertainty assessment

Five types of model assumptions are identified in (Everdij and Blom, 2002) that influence the bias and uncertainty for a target operational concept:

I. Differences in the operational concept used in the model and the target operational concept
II. Non-coverage of hazards
III. Model structure
IV. Parameter values
V. Numerical approximations.

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

- *Bias*. Due to the adoption of the formal model assumptions, 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.

Based on the results of a bias and uncertainty assessment for the ATC routine monitoring operational concept (Everdij and Blom, 2002) and ACAS results (Hawkes, 1998; Arino et al., 2002), an overview of the assumptions which have the strongest effect on the bias in the accident risk is provided in Table 8. An overview of the assumptions regarding the parameters which have the strongest effect on the uncertainty in the accident risk at S=13.5 NM is provided in Table 9.

Table 8 Assumptions that have a major, significant or minor effect on the bias. Optimistic/pessimistic indicates that the accident risk is expected to be lower/higher due to the assumption. Major is about a factor 10, significant is about a factor 2.25, minor is about a factor 1.5.

Assumption	Type	Effect
No semi-circular use of route structure	I	Major Pess.
Aircraft are not TCAS equipped	I	Sign. Pess.
There is no STCA system	I	Sign. Pess.
Standard deviation of lateral deviation after ATCo unexpected sharp turn	IV	Sign. Opt.
There are no party line effects	II	Minor Pess.
ATCo neglects secondary conflicts when giving an avoidance instruction	II	Minor Pess.
Ground aircraft tracking uses alpha-beta filter and single radar coverage only is considered	II	Minor Pess.
Pilot performance mode is independent of modes of technical systems or ATCo	III	Minor Opt.
Aircraft flightplan is independent of human operators or technical systems, except ATCo	III	Minor Opt.

Table 9 Main uncertainties in the model risk due to uncertainty in parameter values.

Parameter	Effect
Number of aircraft entering each lane per hour	Significant
Probability of wrong clearance by ATCo in opportunistic control mode	Significant
Maximum ATCo-allowed lateral deviation from lane	Minor
Standard deviation of vertical position of aircraft	Minor
Maximum course deviation during turn of aircraft	Minor
Mean duration of implementing clearances for *Relaxed* pilot	Minor
Mean duration of *No Comm B* by ATCo	Minor
Mean duration of *No Comm C* by ATCo	Minor
Probability of wrong clearance by ATCo in tactical mode	Minor
Number of pending tasks at which control mode of ATCo becomes opportunistic	Minor
Mean duration of transition of aircraft flightplan from *Conform to route* to *Different from route*	Minor
Width of aircraft	Minor
Height of aircraft	Minor

5.2 Expected accident risks and safe spacing

The idea behind the approach is that if one can judge the bias and uncertainty of each individual model assumption conditional on all previous assumptions, and is able to combine these results, one can estimate the bias and uncertainty in model-based accident risk due to all assumptions adopted. Next, one can determine an estimate for operational concept accident risk, by compensating for this evaluated bias and uncertainty in the model-based accident risk. The combined bias and uncertainty results are now added to the collision risk curve (see Figure 7). At S=13.5 NM the actual risk is expected to be 3.5 times smaller than the modelled risk. The 95% credibility interval has been assessed to range from a factor 4.5 higher to a factor 12.2 lower than the expected risk. It seems reasonable to assume that the bias and uncertainty correction applies for values of $S > 8$ NM. Then from Figure 7 we may conclude that for the operation considered a safe spacing value S=11 NM results for the ATC example considered.

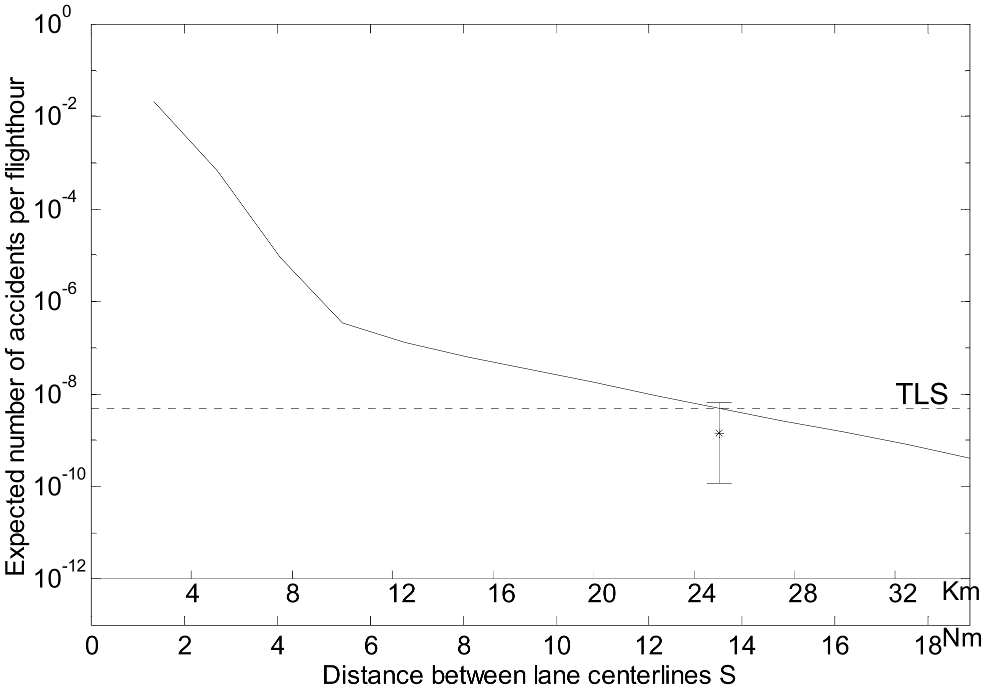

*Figure 7 ATC routine monitoring model-based accident risk curve (continuous line) and expected accident risk at S=13.5 NM (denoted by *). The bar indicates the 95% credibility interval at S=13.5 NM. TCAS effect is not taken into account by ICAO TLS and neither included in the curve or the 95% accident risk area.*

5.3 Safety criticality analysis

A safety criticality analysis shows which events for a pair of aircraft contribute most to the accident risk for the spacing at which the target level of safety is attained. Analysis for the hypothetical ATC example considered indicates that the most safety critical situation is the one for which (see also Figure 6):

- One aircraft is flying nominally along the flight lane (*Nominal*), and
- The opposite aircraft is making a strong and sudden deviation from the flight lane (*Sharp turn*),
- While the decision making loop (surveillance - controller - communication) is functioning properly for both aircraft, and
- The navigation systems of both aircraft and on the ground are working nominally.

Furthermore, it follows that aircraft with slowly developing deviations from the flight lane (*Non-nominal* evolution mode), due to degraded navigation systems or degraded aircraft systems, have a smaller impact on the collision risk, although the probability of *Non-nominal* evolution exceeds the probability of *Sharp turn* evolution. *Sharp turn* evolution is caused by an erroneous controller clearance or an aircraft flightplan error, whereas the *Non-nominal* deviations are largely caused by degraded technical systems. Hence, from the safety criticality analysis we may conclude that the most safety critical situations are related to intent mismatches between pilots and controller rather than to degraded performance of technical systems.

6 Conclusions

When designing advanced ATC, it is important to understand the safety issues already at a conceptual level. Because of the extremely low probability of accidents in existing ATC practice, statistical data from practical situations is limited and analysing accident reports alone is not sufficient to understand safety at the level of the interactions between the various ATC components. For advanced ATC designs, data concerning unsafe events may even be lacking at all. Therefore, some kind of modelling approach is required to optimise for capacity and separation criteria without compromising safety.

Since in about 80% of the reported accidents humans were part of the cause, it is imperative to properly incorporate the human factor into the models used for risk assessment. In this paper, we therefore investigated three complementary psychological models, and we combined them into a single mathematical model of a tactical controller in a conventional en-route context. Because monitoring activity is typically performed as an integrated part of the tactical controller job, it is necessary to also take into account other controller activities that may interfere with monitoring. This was accomplished through our contextual model of controller performance that takes into account the interfering tasks at a cognitive level, thus minimising the level of modelling detail required to take into account the interfering tasks. This model is shown to be of great use in the evaluation of both controller cognitive performance and accident risks, when evaluating ATC concepts. We also showed that this advanced controller performance model can be used to evaluate ATC concepts from the level of controller performance up to the level of accident risk.

We conclude that the use of advanced psychological models in accident risk modelling is feasible, thus extending the applicability of the accident risk modelling approach to situations where isolated models of individual human actions do not suffice.

References

AGARD (1998). *A designer's guide to human performance modelling*. AGARD Advisory report 356.

Amalberti, R. and Wioland, L. (1997). Human error in aviation. In, H. Soekkha (Ed.), *Aviation Safety* (pp. 91-108). Zeist, NL: VSP International Science Publishers.

Ammerman, H.L., Fairhurst, W.S., Hostler, C.M. and Jones, G.W. (1987). *FAA air traffic control concepts volume VI: ARTCC/HOST en route controllers.* DOT/FAA/AP/87-01 Report. Washington DC: FAA

Arino, T., Carpenter, K., Chabert, S., Hutchinson, H., Miquel, T., Raynaud, B., Rigotti, K. and Vallauri, E. (2002). *ACAS - Final report on the full system safety study.* Report CENA, QinetiQ, Sofreavia.

Bainbridge, L. (1993). The change of concepts needed to account for human behaviour in complex dynamic tasks. *Proceedings of 1993 International Conference on Systems, Man and Cybernetics*, *1,* 126-131

Blom, H.A.P., Everdij, M.H.C. and Daams, J. (1999). *Modern Safety Cases for a new operation in air traffic, Part II*. NLR Report, *http://www.nlr.nl/public/hosted-sites/ariba/*

Blom, H.A.P., Bakker, G.J., Blanker, P.G.J, Daams, J., Everdij, M.H.C. and Klompstra, M.B. (2001a). Accident risk assessment for advanced air traffic management. In, G.L. Donohue and A.G. Zellweger (Eds.), *Air Transport Systems Engineering* (pp. 463-480). Washington DC: AIAA.

Blom, H.A.P., Daams, J. and Nijhuis, H.B. (2001b). Human cognition modelling in ATM safety assessment. In, G.L. Donohue and A.G. Zellweger (Eds.), *Air Transport Systems Engineering* (pp. 481-511). Washington DC: AIAA.

Blom, H.A.P., Stroeve, S.H., Everdij, M.H.C. and Van der Park, M.N.J. (2002). Human cognition performance model based evaluation of safe spacing in air traffic. In, *Proceedings 23rd International Congress of Aeronautical Sciences*, Toronto, Canada, 8-13 September 2002

Buck, S., Biemans, M.C.H., Hilburn, B.G. and Van Woerkom, P.T.L.M. (1996). *Synthesis of functions*. NLR Report TR-970545L. Amsterdam: NLR.

Cohen, S. and Hockaday, S. (Eds.) (1998). *A concept paper for separation safety modelling*. FAA/ Eurocontrol Report

Corker, K.M. (2000). Cognitive models and control: Human and system dynamics in advanced airspace operations. In, N. Sarter and R. Amalberti (Eds) *Cognitive engineering in the aviation domain* (pp. 13-42). Mahwah, NJ: Lawrence Erlbaum Associates.

Cox, M. (1994). *Task analysis of selected operating positions within UK air traffic control*. RAF Institute of Aviation Medicine, Report No. 749.

Daams, J., Blom, H.A.P. and Nijhuis, H.B. (2000). Modelling human reliability in air traffic management. In, *Proceedings of 5th Probabilistic Safety Assessment and Management Conference* (pp. 1193-1198). Osaka, Japan,

EATCHIP (1996). *Model for Task and Job Descriptions of Air Traffic controllers*. Report HUM.ET.ST01.1000-REP-01. Brussels: Eurocontrol.

Endsley MR, Rodgers MD (1994). *Situation awareness information requirements for en route air traffic control*. Texas Univ.

Everdij, M.H.C. and Blom, H.A.P. (2000). *Piecewise deterministic Markov processes represented by Dynamically Coloured Petri Nets*. Report NLR-TP-2000-428. Amsterdam: National Aerospace Laboratory NLR.

Everdij, M.H.C. and Blom, H.A.P. (2002). *Bias and uncertainty in accident risk assessment.* Report NLR TR-2002-137. Amsterdam: National Aerospace Laboratory NLR.

Rodgers, M.D., Mogford, R.H. and Mogford, L.S. (1998). *The relationship of sector characteristics to operational errors*. FAA report DOT/FAA/AM-98/14. Washington DC: US DoT.

Haraldsdottir, A., Schwab, R.W. and Alcabin, M.S. (2001). Air Traffic Management Capacity Driven Operational Concept Through 2015. In, G.L. Donohue and A.G. Zellweger (Eds.) *Air Transport Systems Engineering* (pp. 9-25). Washington DC: AIAA,

George, P.H., Johnson, A.E. and Hopkin, V.D. (1973). *Radar monitoring of parallel tracks, automatic warning to controllers of track deviations in a parallel track system*. EEC Report No 67, Bretigny-sur-Orge.

Hawkes, D. (1998). *Airborne Collision Avoidance Systems II (ACAS II)*. Joint Aviation Authorities, Position paper 017_12

Hollnagel, E. (1993). *Human Reliability analysis, context and control*. London: Academic Press.

ICAO (1998). *Annex 11 - Air Traffic Services, 12th edition, incorporating amendments 1-38, Green pages, attachment B, paragraph 3.2.1*

Isaac, A., and Ruitenberg, B. (1999). *Air traffic control: human performance factors*. Aldershot: Ashgate

Jackson, A. (1989). *The role of the controller in future ATC systems with enhanced information processing capabilities*. EEC report No 224

Kilner, A., Hook, M. and Duck, R. (1997). *Workload Assessment*. Report TOSCA II WPR/8/01 Part I, NATS

Kirwan, B. (1994). *A guide to practical human reliability assessment.* London: Taylor and Francis

Odoni, A.R. et al. (1997). *Existing and required modelling capabilities for evaluating ATM systems and concepts.* Cambridge, MA: MIT.

Stroeve, S.H., Van der Park, M.N.J., Everdij, M.H.C. and Blom, H.A.P. (2002). *Mathematical model used for TOPAZ evaluations in DADI*. NLR Memorandum LL-2000-004.

Stroeve, S.H., Blom, H.A.P., Van der Park, M.N.J. and Everdij, M.H.C. (2003). Improved bias and uncertainty assessment in accident risk assessment. NLR Memorandum LL-2003-013.

Wickens C.D. (1992). *Engineering, Psychology and Human Performance*. Columbus: Merrill.

Wickens C.D., Mavor A.S., Parasuraman R. and McGee J.P. (Eds.) (1998). *The future of Air Traffic Control, Human Operators and Automation*. Washington, DC: National Academy Press.

Appendix A Acronyms

AGARD	Advisory Group for Aerospace Research and Development
ATC	Air Traffic Control
ATCo	Air Traffic Controller
DCPN	Dynamically Coloured Petri Net
DM-loop	Decision Making loop
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme
FMS	Flight Management System
ICAO	International Civil Aviation Organisation
NM	Nautical Mile
R/T	Radio Telephony
RNP1	Required Navigation Performance (95% of time within 1 NM)
STCA	Short Term Conflict Alert
TCAS	Traffic alert and Collision Avoidance System
TLS	Target Level of Safety