



NLR-TP-2006-694

## **The roles of air traffic controllers and pilots in safety risk analyses**

H.H. de Jong, S.H. Stroeve and H.A.P. Blom

This report contains a paper in Proceedings ESREL 2006, 22-26 September 2006, Estoril, Portugal.

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 <i>18.12.2006</i> 	Reviewer Anonymous peer reviewers	Managing department  <i>22/12/06</i>
--	--------------------------------------	--

# The roles of air traffic controllers and pilots in safety risk analyses

Hans H. de Jong, Sybert H. Stroeve & Henk A.P. Blom

*National Aerospace Laboratory NLR, Amsterdam, The Netherlands*

**ABSTRACT:** Air traffic controllers and pilots are crucial in achieving high levels of safety in air traffic operations. Their performance is consequently an essential subject of safety risk analyses, which need to be executed when advanced air traffic operations are developed. The paper describes a systematic and stepwise approach to safety risk analysis, which is integrated in the development of advanced air traffic operations. The approach recognizes and exploits the ability of air traffic controllers and pilots to provide operational expertise necessary to perform such analyses. The roles of air traffic controllers and pilots in the safety risk analysis steps are elaborated by means of an application for a proposed air traffic operation at Amsterdam Airport Schiphol in which taxiing aircraft pass an active runway. Controllers and pilots have the following important roles in safety risk analysis and operational development: pushing the boundary between imaginable and unimaginable hazards in hazard identification, providing expert knowledge for argumentation-based and Monte Carlo simulation-based safety risk analysis, identifying potential mitigating measures, and providing a basis for acceptance of the introduction of an advanced operation.

## 1 INTRODUCTION

For effective development of advanced air traffic operations, safety risk analysis forms a primary source of feedback to assure that safety risks at the air traffic capacity-level required are acceptable. Early guidance of operational development on safety grounds can help to avoid a potentially costly redevelopment programme. Moreover, analysis of safety risk against appropriate safety criteria is a requirement for implementation of advanced operations; see for instance (EC Commission, 2005; Eurocontrol, 2001). Apostolakis (2004) provides a perspective on the usefulness of quantitative risk assessments.

Given the crucial roles of air traffic controllers and pilots in maintaining safety of air traffic operations, their performance is an essential part of such safety risk analyses. In line with this, air traffic controllers and pilots provide expertise that is crucial to perform the analyses. In this article, the various roles of air traffic controllers and pilots in safety risk analyses are discussed by means of an example operation in which taxiing aircraft cross the active Runway 18C/36C at Amsterdam Airport Schiphol.

The organization of the paper is as follows:

- Section 2 outlines the steps in a safety risk analysis and indicates for which steps the roles of air traffic controllers and pilots will be addressed;

- Section 3 sketches an operation that will be used to illustrate the approach;
- Section 4 and 5 focus on the role of controllers and pilots in hazard identification and argumentation-based safety risk analysis;
- Section 6 outlines the use of simulation-based safety risk analysis, simulation of controller and pilot activities and the use of operational expert knowledge in such analyses;
- Section 7 briefly addresses the necessity of controller and pilot involvement in providing feedback to the operational developers;
- Section 8 addresses other aspects of the involvement of operational experts in safety risk analyses; and
- Section 9 presents the conclusions.

## 2 SAFETY RISK ANALYSIS STEPS

This section indicates a generic safety risk analysis cycle for development of advanced air traffic operations (Blom et al., 2006). The steps in the safety risk analysis cycle are shown in Figure 1.

In step 0, the objective of the analysis is determined, as well as the safety regulatory context, scope and level of detail of the analysis. Next, the operation to be assessed is determined (step 1). The actual safety risk analysis starts by identifying

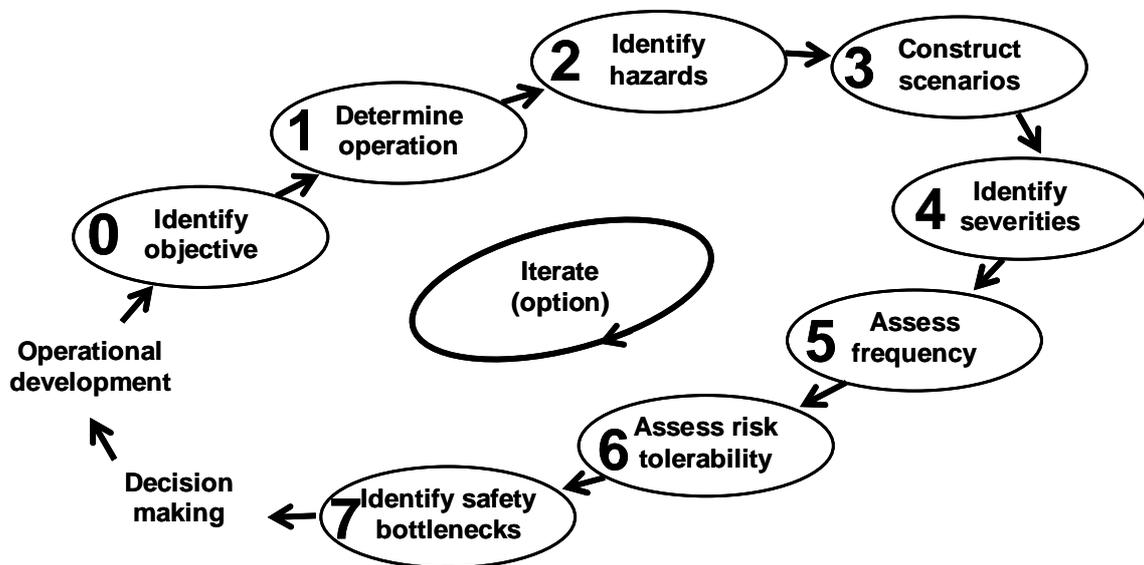


Figure 1: Safety risk analysis cycle

hazards associated with the operation (step 2), and aggregating these into safety relevant scenarios (step 3). Using severity and frequency assessments (steps 4 and 5), the safety risk associated with each safety relevant scenario is classified (step 6). For each safety relevant scenario with a (possibly) unacceptable safety risk, the hazards and/or conditions contributing to insufficient safety, named safety bottlenecks, are identified (step 7). This safety feedback supports operational concept developers to identify for which safety issues they should develop improvements in the operational design. If the design is changed, it is verified by another safety risk analysis cycle whether safety has improved sufficiently. This apparently laborious way to analyse changes to an operation is necessary since the changes may have introduced new hazards or increased the risk of scenarios with previously acceptable safety risk. Such unintentional consequences of changes are easily missed by looking only at the previously unacceptable scenario.

The safety risk analysis methods used in these steps may depend on particular aspects of the safety relevant scenario and the iteration number in the safety risk analysis cycle. This variety in safety risk analysis methods is most prominent in step 5 (assess frequency). In step 5, for each possible severity outcome of a safety relevant scenario, the occurrence frequency is evaluated via an appropriate tree, which describes the probability of the top event in the tree as a sum of a product of probabilities of applicable conditional events. In a first iteration cycle, the factors in this tree are usually assessed by argumentation-based evaluation, for which the primary sources of data stem from interviews with operational experts and safety databases. In subsequent iteration cycles, the quality of the risk estimate may be improved by using dedicated Monte Carlo simulations, which are based on a stochastic dynamic model of the operation.

This paper explains the role of controllers and pilots in the safety risk analysis cycle:

- Pushing the boundary between imaginable and unimaginable hazards in hazard identification (step 2);
- Providing expert knowledge for argumentation-based and Monte Carlo simulation-based safety risk analysis (especially step 5);
- Identifying potential mitigating measures (step 7); and
- Providing a basis for acceptance of the introduction of an advanced operation as representative of the operation's key users (supports decision making step).

### 3 EXAMPLE OPERATION

The safety risk analysis cycle and the roles of controllers and pilots therein are illustrated by an analysis applied to an active runway crossing operation at Amsterdam Airport Schiphol. In this operation, Runway 18C/36C is used for departures or arrivals, whereas taxiing aircraft have to pass it on their ways to or from Runway 18R/36L. See Figure 2 for Runway 18C/36C with surrounding taxiways.

During the development of the infrastructure and the operation, the air traffic control provider and the airport have initially considered crossings over Runway 18C/36C, in order to keep the taxi times between the airport centre and the far-off Runway 18R/36L as low as possible. However, safety risk analysis of this operation yielded potentially dangerous situations (hazards) that had not played a role in the development of the operation up to then. The identification of these hazards was therefore considered very valuable by the developers of the operation. Because of these and other findings, the operation has been developed further.

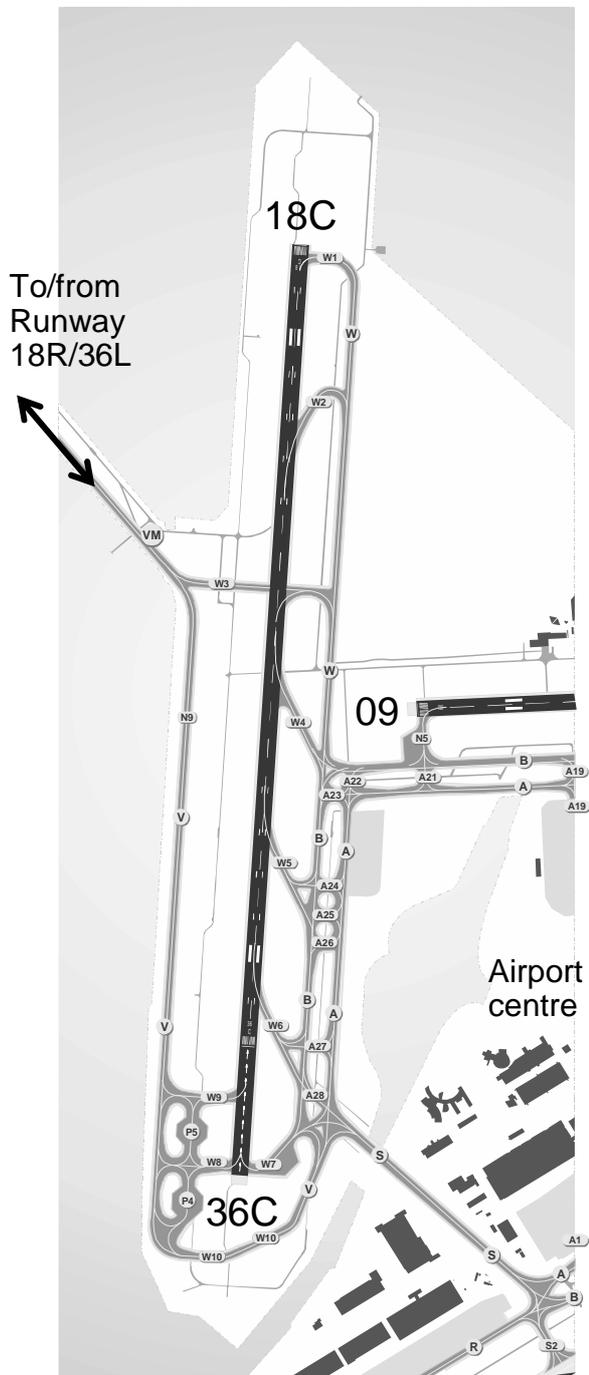


Figure 2: Runway 18C/36C with surrounding taxiways

In the currently considered operation, taxiing to and from Runway 18R/36L takes place via a southern taxiway (see below “36C” in Figure 2). Taxiing cannot be performed independently in case there is traffic landing on Runway 18C/36C from the south, or taking off to the south. The air traffic controller for Runway 18C/36C is responsible for safe dependent taxiing on the southern taxiway. The controller gives permission to use the southern taxiway by means of an instruction to the pilots of the taxiing aircraft in combination with switching off a red stopbar.

#### 4 HAZARD IDENTIFICATION

The term hazard is defined in a wide sense; i.e., an

event or situation with possibly negative effects on safety. Such a non-nominal event or situation may evolve into danger, or may hamper the resolution of the danger, possibly in combination with other hazards or under certain conditions. In step 2 of the safety risk analysis cycle, hazard identification brainstorming sessions are used as primary means to identify hazards. Identification of as many as possible hazards is a prerequisite for a good safety risk analysis. After all, hazards that are left unidentified may lead to a too optimistic safety perspective.

In system engineering, the functional approach to hazard identification is well-known. This approach attempts to determine all possible failure conditions and their effects, for each function that plays a role in the operation, including the human operator tasks. Unfortunately, the approach cannot identify all hazards related to an operation that involves human operators. An important reason for this is that the performance of air traffic controllers and pilots depend on their (subjective) situational awareness. From a human cognition perspective a particular act by an air traffic controller or pilot can be logical, whereas from a function allocation perspective the particular act may be incorrect. Such occurrences are often called “errors of commission” (Sträter et al., 2004). An example of an error of commission in the crossing operation is that, because of the complicated taxiway structure, a pilot thinks that he is still taxiing far from the runway, whereas in reality he already crosses the runway without noticing any of the runway signs.

Another well-known technique of hazard identification is the HAZOP (HAZard and OPerability) method. With this method, hazards are identified and analyzed using sessions with operational experts. At the same time, the experts come up with potential solutions and measures to cope with the identified hazards (Kirwan & Ainsworth, 1992). The advantage of HAZOP with respect to the functional approach is that also non-functional hazards are identified. However, in applying HAZOP, one needs to take care that hazard analysis and solution activities do not disturb the hazard identification process, which could leave hazards unidentified. Moreover, one needs to be aware that potential solutions may introduce new hazards.

With the experience of a large number of safety risk analyses for air traffic operations, and on the basis of knowledge from other safety-critical industries, a method for shifting the boundary between imaginable and unimaginable hazards for air traffic operations has been developed in a study for EUROCONTROL (De Jong, 2004). Subsequently, this method has been incorporated in Version 2 of EUROCONTROL’s Safety Assessment Methodology (EUROCONTROL, 2005).

The method involves pure brainstorming sessions with air traffic controllers and pilots. In such sessions no analysis is done and solutions are not identified. One needs to perform brainstorming sessions with an air traffic controller and pilot that are able to play devil's advocates. It is important to help and not to suppress identification of seemingly remote hazards; they may turn out to bear significant risk after careful analysis or may trigger identification of other more relevant hazards.

Besides the aforementioned error of commission, some hazards for the example operation identified by the pure brainstorming approach are:

- Controllers abuse the alerting system for efficiency reasons; and
- A pilot has counted down the prescribed wake vortex separation time with the previous take-off and he starts to take off without clearance.

## 5 EXPERT KNOWLEDGE IN ARGUMENTATION-BASED SAFETY RISK ANALYSIS

The identified hazards are structured into safety relevant scenarios, which comprise bundles of event/condition sequences and their effects (step 3 in Figure 1). These scenarios are usually centred around a general situation with potential safety effects, such as a conflict between an aircraft taking off and a taxiing aircraft approaching the runway. Subsequently, for each of the safety relevant scenarios, it is determined which severity categories apply to its possible effects (step 4) and for each possible severity category the frequency of occurrence is evaluated (step 5).

Operational experts again play a crucial role in the safety risk analysis by answering questions such as:

- How often does a given hazard occur? In the crossing operation, example hazards are a runway incursion or a take-off without clearance; and
- How likely is it that such a situation results in an incident? How large is, for instance, the conditional probability that an air traffic controller detects and resolves an imminent runway incursion?

Such questions are often difficult to answer. After all:

- For advanced operation designs there is usually little relevant experience;
- An operation includes many agents (e.g., pilots, controllers, navigation systems, alert systems), which interact with each other, making the outcomes of scenarios difficult to analyse; and
- Hazardous situations may occur so rarely that relevant statistical data is not available.

Therefore it is often hard to give direct quantitative estimates of expected occurrence frequencies. A way to proceed is to identify the relevant operational expertise for the current operation, supplement it with statistical data and use expert judgement and argu-

mentation to extrapolate to the advanced operation. Hence, controllers and pilots remain crucial sources of information. They are asked how often they have experienced situations similar to those under assessment in their careers, to give indications of likelihood and timeliness of detecting and resolving conflicts and to argue and estimate how all of this would change in the advanced operation.

A challenge in using operational expert judgement is that different experts generally give different estimates. The question is how to combine answers of different experts; one expert will probably give more realistic estimates than the other, perhaps some experts are too optimistic and others too pessimistic. (Cooke & Goossens, 2000) give principles for good usage of expert judgement and an approach to "calibrate" experts using questions with known answers, for instance from statistics. In this way, one can account for experts estimating systematically too high or too low, and assign a larger weight to experts whose estimates usually corroborate well with facts than to experts whose estimates are further off. This approach yields better estimates with substantiated uncertainty margins. The principles for good usage have been applied in the safety risk analyses performed, but it turns out that calibration is not always feasible, as this may need more experts than available.

One of the findings obtained in the argumentation-based analysis of the example operation is that radiotelephony communication between controllers and pilots is a safety bottleneck:

- The "lost" pilots (recall the error of commission example) might not even be on the right frequency, making quick resolution of an impending runway incursion by controllers very difficult; and
- Even for pilots on the right frequency, the chance of an occupied frequency severely limits the controllers' effectiveness in resolving (impeding) runway incursions.

## 6 SIMULATION-BASED SAFETY RISK ANALYSIS

As noted in the last section, assessing the frequency of a severity category on the prime basis of expert judgement may be complicated by lack of experience with the designed operation and by dynamic interaction of various agents (e.g., pilots, controllers, technical systems). Assessment of such difficult safety relevant scenarios can be supported by Monte Carlo simulations (Stroeve et al., 2003; Blom et al., 2006). Such Monte Carlo simulations represent the relevant aspects of the operation, including aircraft trajectories, technical systems, procedures and the performance of air traffic controllers and pilots. Nominal as well as non-nominal situations are repre-

sented, in which the latter category uses the knowledge generated by hazard identification brainstorming.

Consider for example the analysis of the probability of a collision between an aircraft departing from a runway while a taxiing aircraft approaches the runway, for instance because it has entered a wrong taxiway. In the model used for the analysis, the runway controller performs a number of tasks. As a result of this, he is able to detect the conflict within a particular period of time and he will usually instruct the pilots, after a period depending among other things on the state of the communication systems. In reaction to such an instruction, the pilots will attempt to prevent a possible accident, for instance by braking. In addition to conflict detection via the controller, the traffic situation is also observed by the pilots, who may detect and react to a conflict as well. These processes of the controllers and pilots are performed in parallel and they depend on the actual traffic situation and the state of the relevant technical systems in the model. This involves the contextual control modelling of (Hollnagel, 1993).

The simulated activities of a controller or pilot for a given traffic situation are based on an analysis of the tasks of these operators, a clustering of these tasks for the mathematical model and an identification of priorities and possibilities to execute these task clusters simultaneously, given the traffic situation (Daams et al., 2000). Examples of task clusters for an air traffic controller are:

- Monitoring: observation of the traffic situation;
- Communication: communication of a clearance; and
- Co-ordination: co-ordination with other air traffic controllers.

In the model, aspects such as conditions to begin an activity, the duration of an activity, its effects and its dependence on the workload and the traffic situation are represented.

The simulations represent the perception of the traffic situation and the related technical systems, operations and their interaction. Perception comprises observation and interpretation of the present and upcoming traffic situation and aspects related to this. As a result of the interaction between the various operators and technical systems in the simulations via processes such as observation and communication, inconsistencies can arise between the traffic pictures of the operators and/ or technical systems. These inconsistencies are typical examples of causes of errors of commission, because each operator and each technical system acts according to its own traffic picture. See (Corker, 2005; Blom et al., 2003) for more general accounts of human performance modelling in the context of air traffic operations.

For operations as complex as the active runway example considered, a simulation model will always differ from reality. Hence, validation of the Monte Carlo simulation results does not mean that one should try to show that the model is perfect. Rather one should identify the differences between the simulation model and reality, and subsequently analyse what the effects of these differences are in terms of *bias* and *uncertainty* at the assessed risk level of the model (Everdij et al., 2006). Thinking in terms of these differences makes it possible to consider the validation problem as a problem of making the differences specific, assessing each difference and its effect on the collision risk, and subsequently decide whether this is sufficiently accurate (valid) or not (invalid) for the purpose. With this approach, the validation of a simulation-based accident risk analysis has largely become a bias and uncertainty assessment process. This process includes identification of differences between the simulation model and reality, assessment of the size of these differences, assessment of the risk sensitivity for differences, and assessment of the joint effect of these differences.

In attaining feedback on the differences between model and reality in the bias and uncertainty assessment process, interviews with pilots and controllers play an important role. For the crossing operation example, a first analysis of the possible effects of such differences showed that the more important differences are related to task handling, conflict detection and conflict resolution of pilots and controllers. Questions in the interviews with pilots and controllers interviews for assessment of these differences cover for instance the duration of performing tasks, reaction times, angles of view and the effects of actions to prevent collisions. On the basis of the answers of the operational experts, statistical data and additional Monte Carlo simulations, the expected accident risk and the uncertainty therein are given.

For the example operation, the simulation-based analysis has made clear that although the runway controller identifies a good share of the conflicts, the contribution to timely resolution is relatively small. A significant part of the resolution instructions by the controller concerns conflicts already solved by pilots; another part of the instructions appears too late for the pilots to avoid successfully a collision. (This is partly because of the radio-telephony safety bottleneck mentioned before.) These dynamic aspects are very difficult to handle well in a purely argumentation-based analysis.

## 7 FEEDBACK TO DECISION MAKING AND OPERATION DEVELOPMENT

Evaluation of the combined severity and frequency assessments (steps 4 and 5 in Figure 1) with the risk criteria provides the risk tolerability of the safety relevant scenarios (step 6). For scenarios with (possibly) unacceptably high risk, the hazards and/or conditions that contribute most to the high risk level or its confidence interval are identified in step 7. These hazards and conditions are referred to as safety bottlenecks and they are important as they give developers of the advanced operation clues for searching potential risk mitigating measures of the operation. For scenarios in which unacceptable risk is possible in relation to large uncertainties, the safety bottlenecks indicate to the safety risk analysis experts where reduction of uncertainty has priority.

Like identification of hazards, experience has taught that identification of mitigating measures cannot be done well only by engineers behind their desks. Operational expertise is necessary to be creative in identifying potential mitigating measures for safety-critical aspects and to get measures that would work in practice.

A simple mitigating measure quickly identified for the example operation was to introduce traffic signs stating the correct radiotelephony frequency.

Apart from risk being acceptable or at least tolerable according to appropriate safety criteria, support of the prospective users of the operation (pilots and air traffic controllers) is crucial for introduction of an advanced operation. Management will have a very hard time introducing an operation if the operational experts do not support it. The endorsement of controllers and pilots of the safety risk analysis is a considerable step towards their support. In this way, operational experts indirectly play an important role in the decision-making process for the design and implementation of an advanced operation. To facilitate acceptance of the safety risk analysis' results, the air traffic controllers and pilots involved in the safety risk analysis need to understand and trust the process of the safety risk analysis. They need to be a good sample of and well respected by the groups of operational experts they represent.

## 8 CHALLENGES IN USING OPERATIONAL EXPERTS

The previous sections have indicated crucial roles of air traffic controllers and pilots in several steps in safety risk analysis. This section gives some further advice on how to make the best use of operational experts in safety risk analyses.

In the first place, air traffic controllers and pilots are professionals usually heavily occupied with their primary tasks. Consequently, they may not be easy

to arrange for involvement in safety risk analyses. The importance of operational experts for safety risk analyses has to be acknowledged at management level to secure their participation. This obviously needs to be organised at an early stage of the safety risk analysis.

The safety risk analysis needs to involve air traffic controllers and pilots who have as much as possible up-to-date experience with current operations. The analysis of advanced operations becomes more difficult, if the experience of the operational experts is less in line with the latest developments, making the gap to the advanced operation even larger. Furthermore, the acceptance of the safety risk analysis' results by the general community of controllers and pilots is promoted better if the operational experts are actively involved in current air traffic operations.

For hazard identification, air traffic controllers and pilots able to play devil's advocates are necessary.

The operational experts involved in the argumentation-based safety risk analysis (in particular the frequency assessment) and the simulation-based analysis (in particular the assessment of the modelling assumptions made) need to be able to look further than their personal experience (to be able to estimate frequencies of rare events) and to be able to imagine how they would handle in such events. Large differences in the operational experts' horizons of imagination have been experienced. Although the various tasks in safety risk analyses ask for slightly different characteristics of controllers and pilots, it is advised to involve a fixed group of these experts through the whole analysis. This minimizes the total time that needs to be spent on introducing these experts to the advanced operation and explaining the process of the analysis and their role therein, and it allows the involved group to get a comprehensive picture of the analysis.

## 9 CONCLUSIONS

In this article, it is explained that air traffic controllers and pilots have a clearly discernable role in most steps of the safety risk analysis of air traffic operations:

- Shifting the boundary between imaginable and unimaginable hazards;
- Contribution of expert knowledge in argumentation-based analysis;
- Contribution of expert knowledge for the simulation model and assessment of model assumptions;
- Facilitate acceptance of introduction of advanced operations by serving as representatives of the users of the operation; and
- Identification of potential mitigating measures in case the safety risks of the advanced operation are not all acceptable.

## REFERENCES

- Apostolakis GE (2004). How Useful Is Quantitative Risk Assessment? *Risk Analysis* 24(3)
- Blom HAP, Stroeve SH, Everdij MHC & Van der Park MNJ (2003). Human cognition performance model to evaluate safe spacing in air traffic. *Human Factors and Aerospace Safety* 3(1): 59-82
- Blom HAP, Stroeve SH & De Jong HH (2006). Safety Risk Assessment by Monte Carlo Simulation of Complex Safety Critical Operations. In Redmill F & Anderson F (eds.), *Proc. of the 14th Safety critical Systems Symposium*, Bristol, UK, February 2006, Springer
- Cooke RM & Goossens LJH (2000). Procedure guide for structured expert judgement. *Project report for EURATOM*, European Commission EUR 18820 EN
- Corker KM (2005). Computational Human Performance Models and Air Traffic Management. In Kirwan B, Rodgers M & Schäfer D (eds.), *Human Factors impacts in air traffic management*, Ashgate Publishing Limited, pp. 317-350
- Daams J, Blom HAP & Nijhuis HB (2000). Modelling Human Reliability in Air Traffic Management. *Proceedings of Fifth Probabilistic Safety Assessment and Management Conference*, Osaka, Japan, 27 Nov – 1 Dec 2000: pp. 1193-1198
- De Jong HH (2004). Guidelines for the identification of hazards; How to make unimaginable hazards imaginable? *NLR Contract report for EUROCONTROL*, NLR-CR-2004-094, March 2004, hdejong@nlr.nl
- EC Commission (2005). Commission Regulation (EC) No 2096/2005 laying down common requirements for the provision of air navigation services, Official Journal of the European Union, L 335/13-30, 21 December 2005, [http://europa.eu/eur-lex/lex/LexUriServ/site/en/oj/2005/l\\_335/l\\_33520051221en00130030.pdf](http://europa.eu/eur-lex/lex/LexUriServ/site/en/oj/2005/l_335/l_33520051221en00130030.pdf)
- Eurocontrol (2001). Safety Regulatory Requirement - ESARR 4, Risk Assessment and Mitigation in ATM, Edition 1.0, 5 April 2001, <http://www.eurocontrol.int/src/gallery/content/public/documents/deliverables/esarr4v1.pdf>
- Eurocontrol (2005). Safety Assessment Methodology, Version 2.0, April 2005, Patrick Mana (contact person), [http://www.eurocontrol.int/safety/gallery/content/public/library/SAM/SAM\\_Electronic\\_V2.0.zip](http://www.eurocontrol.int/safety/gallery/content/public/library/SAM/SAM_Electronic_V2.0.zip)
- Everdij MHC, Blom HAP & Stroeve SH (2006). Structured Assessment of Bias and Uncertainty in Monte Carlo Simulated Accident Risk. *Proc. 8<sup>th</sup> Int. Conf. on Prob. Safety Assessment and Management*, New Orleans, US, 14-19 May 2006
- Hollnagel E (1993) *Human reliability analysis: context and control*. London, Academic Press
- Kirwan B & Ainsworth LK (1992) *A guide to task analysis*. Taylor and Francis
- Sträter O, Dang V, Kaufer B & Daniels A (2004) On the way to assess errors of commission. *Reliability Engineering and System Safety* 83: 129-138
- Stroeve SH, Blom HAP & Van der Park MNJ (2003). Multi-agent situation awareness error evolution in accident risk modelling, *Proceedings of the 5th USA/Europe ATM R&D Seminar*, Budapest, Hungary, 23 – 27 June 2003