

Executive summary

SYSTEMIC ACCIDENT RISK ASSESSMENT IN AIR TRAFFIC BY MONTE CARLO SIMULATION

Problem area

Air traffic risk assessments have predominantly been done by sequential and epidemiological accident models, such as fault and event trees. These types of models have limitations in representing dependent dynamics in air traffic scenarios. A systemic accident model considers accidents as emergent phenomena from variability and interactions in a complex system. As such it is better suited for risk assessment of complex scenarios in air traffic.

Description of work

In this paper we demonstrate that Monte Carlo simulation of safety relevant air traffic scenarios is a viable approach for systemic accident assessment. The Monte Carlo simulations are based on dynamic multi-agent models, which represent the distributed and dynamic interactions of various human operators and

technical systems in a safety relevant scenario. The approach is illustrated for a particular runway incursion scenario, which addresses an aircraft taxiing towards the crossing of an active runway while its crew has inappropriate situation awareness.

Results and conclusions

An assessment of the risk of a collision between the aircraft taxiing with an aircraft taking-off is presented, which is based on dedicated Monte Carlo simulations in combination with a validation approach of the simulation results. The assessment particularly focuses on the effectiveness of a runway incursion alert system that warns an air traffic controller, in reducing the safety risk for good and reduced visibility conditions.

Applicability

Safety risk assessment of complex scenarios in air traffic.

Report no.

NLR-TP-2009-194

Author(s)

S.H. Stroeve
H.A.P. Blom
G.J. Bakker

Report classification

UNCLASSIFIED

Date

April 2009

Knowledge area(s)

Vliegveiligheid (safety & security)

Descriptor(s)

Runway incursion
TOPAZ
Systemic accident model
Risk assessment
Dynamic risk modelling
Monte Carlo simulation

NLR-TP-2009-194

SYSTEMIC ACCIDENT RISK ASSESSMENT IN AIR TRAFFIC BY MONTE CARLO SIMULATION

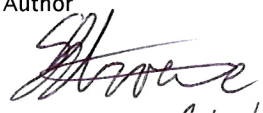
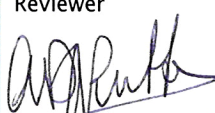
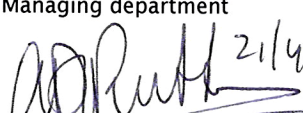
S.H. Stroeve
H.A.P. Blom
G.J. Bakker

This report is based on a paper published in Safety Science 47 (2009), pp. 238-249.

The contents of this report may be cited on condition that full credit is given to NLR and the authors.

Customer	NLR
Owner	NLR
Division	Air Transport
Distribution	Unlimited
Classification of title	Unclassified
	April 2009

Approved by:

Author  21-4-'09	Reviewer  21/4/09	Managing department  21/4/09
---	--	--

SUMMARY

A systemic accident model considers accidents as emergent phenomena from variability and interactions in a complex system. Air traffic risk assessments have predominantly been done by sequential and epidemiological accident models. In this paper we demonstrate that Monte Carlo simulation of safety relevant air traffic scenarios is a viable approach for systemic accident assessment. The Monte Carlo simulations are based on dynamic multi-agent models, which represent the distributed and dynamic interactions of various human operators and technical systems in a safety relevant scenario. The approach is illustrated for a particular runway incursion scenario, which addresses an aircraft taxiing towards the crossing of an active runway while its crew has inappropriate situation awareness. An assessment of the risk of a collision between the aircraft taxiing with an aircraft taking-off is presented, which is based on dedicated Monte Carlo simulations in combination with a validation approach of the simulation results. The assessment particularly focuses on the effectiveness of a runway incursion alert system that warns an air traffic controller, in reducing the safety risk for good and reduced visibility conditions.

CONTENTS

1	INTRODUCTION	7
2	RUNWAY INCURSION SCENARIO	11
2.1	Runway incursion	11
2.2	Aerodrome operation for runway incursion scenario	11
3	SAFETY RISK ASSESSMENT CYCLE	14
3.1	Steps in the safety risk assessment cycle	14
3.2	Safety relevant scenario diagram	15
3.3	Severity and frequency assessment	16
4	MONTE CARLO SIMULATION MODEL	18
4.1	Development of a dynamic stochastic multi-agent model	18
4.2	Overview of the runway incursion model	18
4.3	Parameterisation of the simulation model	22
4.4	Speed-up of Monte Carlo simulation	23
5	MONTE CARLO SIMULATION OF RUNWAY INCURSION	25
6	BIAS AND UNCERTAINTY ASSESSMENT	27
6.1	Validation: assessment of differences between model and reality	27
6.2	Steps in the bias and uncertainty assessment	28
6.3	Bias and uncertainty results for the runway incursion scenario	30
6.4	Potential implications of the risk assessment results	32
7	DISCUSSION	34
8	REFERENCES	38

I INTRODUCTION

In modern large technological organizations, processes often depend on complex and distributed interactions between human operators and technical systems, where the interactions are knowledge intensive and regulated by procedures. A typical example is the air traffic industry, which uses advanced technological systems (e.g. aircraft, communication/navigation/surveillance systems), is knowledge and procedure intensive, and involves interactions between many humans (e.g. pilots, air traffic controllers, airline centre operators).

From a safety assessment point of view, determinants of the complexity of an organization under study include:

- the number and types of entities in the organization (human roles, technical systems);
- the number and types of interdependencies between entities in the organization;
- the degree of distribution of the entities (single/multiple locations);
- the types of dynamic performance of the entities (static/slow/fast);
- the number and types of hazards in the organization, i.e. situations/conditions that potentially affect the level of safety.

In this respect, air traffic stands out as being very complex.

It is argued by Perrow (1984) that as result of the growing complexity of socio-technical systems and the human inability to understand and control those, accidents should be considered natural occurrences rather than abnormal phenomena. Hollnagel (2004) builds further on the notion that accidents are normal occurrences and stresses the role of performance variability for the origin of accidents. He argues that human performance must be variable because of the complexity of the socio-technical environment, and that it is the variability of performance rather than the complexity of systems as such that is the main reason for accidents. As a basis for analysis of performance variability, Pariès (2006) points out that to understand the properties of a complex system, we lay relationships between micro and macro levels, such that macro level properties emerge from assembling micro level properties. In this argumentation, the resilience of a complex organization to recover from mishap emerges from the interactions between the agents in the organization. These views indicate that for managing safety risk and resilience in complex organizations, we need analysis

approaches that account for the variability in their multi-agent performance and the emergence of safety occurrences from this variability.

Hollnagel (2004) categorizes accident models in the following three types, namely two well known and established types of accident models and a third type that is based on above mentioned recent views:

1. *Sequential accident models* describe an accident as the result of a sequence of events that occur in a specific order. These models assume that there are well-defined cause-effect links that propagate the effects of events leading to an accident. Examples of sequential accident models are the domino theory, event trees, fault trees and network models. Many methods used in practice are based on the traditional fault/event tree. However, as argued by Hollnagel (2004) and Sträter (2005), they may not be adequate to account for the complexity of modern socio-technical systems.
2. *Epidemiological accident models* describe an accident in analogy with the spreading of a disease, i.e. as the outcome of a combination of factors, such as performance deviations, environmental conditions, barriers and latent conditions. Like sequential accident models, epidemiological accident models rely on cause-effect propagation in accidents. Examples of epidemiological models are the “Swiss cheese” model of Reason (1997) and Bayesian belief networks. Epidemiological models provide a broader basis to represent the complexity of accidents than sequential models by accounting for more complex interactions between relevant factors.
3. *Systemic accident models* describe the performance of a system as a whole, rather than on the level of cause-effect mechanisms or epidemiological factors. The systemic view considers accidents as emergent phenomena from the variability of a system, for instance due to the dynamic interaction between multiple agents (humans, technical systems), which form a joint cognitive system (Hollnagel and Woods, 2005). Examples of systemic models can be found in control theory and chaos theory. Hollnagel (2004) explains how this may lead to stochastic resonance in a joint cognitive system. Unlike sequential and epidemiological models, systemic models do not rely on fixed cause-effect relations and pass the limitations of sequential and epidemiological models in accounting for the dynamic, non-linear and possibly resonance-like nature of the interactions that may lead to accidents.

For safety assessment of air traffic, the two established types of accident models have been rather well developed. Sequential accident models are commonly known and applied in aviation. Fault and event trees are often applied in system

dependability and safety requirement studies for air traffic (Eurocontrol, 2004a, 2006; EUROCAE, 2000). Epidemiological accident models have recently been used in air traffic safety assessment methods such as the Human Factors Analysis and Classification System (Wiegmann and Shappell, 2001) and Bayesian belief networks for air transport safety (Greenberg et al., 2005; Kardes and Luxhoj, 2005; Ale et al., 2006).

Systemic accident models are less well known for air traffic safety assessment. Nevertheless, in the light of above discussion on risk assessment of complex systems, this type of model is pre-eminently suited to account for the distributed and dynamic nature of air traffic operations in safety assessment. Motivated by stochastic system and control theory, researchers at NLR have developed a methodology for the evaluation of air traffic risk, which coincides well with the systemic accident model view of Hollnagel (2004). This methodology uses Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of air traffic operations. In (Blom et al., 2001a,b, 2003) an initial version of this methodology has been introduced under the name TOPAZ (Traffic Organization and Perturbation AnalyZer). Subsequently, the TOPAZ methodology has been extended with multi-agent situation awareness modelling (Stroeve et al., 2003), an integrated qualitative safety risk assessment cycle (Blom et al., 2006), risk bias and uncertainty assessment (Everdij et al., 2006a), and compositional specification of accident models (Everdij et al., 2006b). Recently, also other researchers have described the behaviour of an air traffic management system as being emergent from the combined actions of individual entities in the system, which can be analysed effectively by agent-based simulations (Shah et al., 2005; Lee et al., 2007).

The aim of this paper is to show that Monte Carlo simulation of safety-relevant scenarios with dynamically interacting agents enables systemic accident risk assessment well. Our example application is a runway incursion scenario, which deals with multiple concurrently interacting human operators and technical systems. In particular, the assessment considers the risk of a collision between an aircraft taking-off with an aircraft taxiing inappropriately across the runway, and focuses on the effectiveness of a runway incursion alert system in reducing the safety risk. The systemic risk assessment approach portrayed in this paper intends to be an effective means to provide feedback to designers of complex air traffic operations.

This paper is organised as follows. Section 2 introduces the runway incursion safety issue and describes the aerodrome operation for which the runway

incursion risk is evaluated. Section 3 describes the safety assessment cycle used for the evaluation of the runway incursion risk and introduces the types of models applied in this cycle. Section 4 describes the Monte Carlo simulation model that is developed for the runway incursion scenario. Section 5 presents the results of the Monte Carlo simulations. Section 6 gives a validation approach of the simulation results, which provides an evaluation of bias and uncertainty in the risk. Section 7 presents a discussion.

An early version of this paper was presented at the Eurocontrol Safety R&D Seminar 2006 (Stroeve et al., 2006).

2 RUNWAY INCURSION SCENARIO

2.1 RUNWAY INCURSION

A runway incursion is defined by the International Civil Aviation Organization (ICAO) as “Any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle or person on the protected area of a surface designated for the landing and take off of aircraft”. Within air traffic, the risk of runway incursion is recognised as an important safety issue. Safety programmes such as (Eurocontrol, 2004b) promote procedures and training to reduce runway incursion risk, such as following ICAO compliant procedures and naming, applying standard radiotelephony (R/T) phraseology, pilot training on aerodrome signage and markings, using standard taxi routes, etc. In addition to procedure and training related measures, research and development is done on new technology in the aircraft, air traffic control (ATC) tower, ground vehicles and aerodrome. Part of these systems aim to reduce the probability of runway incursion by enhancing situation awareness, providing improved guidance on the aerodrome and supporting efficient communication. Other systems aim to reduce the consequences of a runway incursion by alerting one or more involved operators.

In this latter class, runway incursion alert systems directed to the controller are commercially available. False alerts are a well-known problem with such systems. The conditions under which well-functioning ATC runway incursion alerting may be effective are, however, not well known in the safety literature. Assessment of runway incursion risk and of the potential effect of runway incursion risk reducing measures and technologies are demanding tasks, given the large number of human operators, aircraft and supporting technical systems that closely interact on the aerodrome. An analysis with a systemic accident model of a multi-agent runway incursion scenario is considered in this paper.

2.2 AERODROME OPERATION FOR RUNWAY INCURSION SCENARIO

The runway considered is used for departures and has a taxiway that crosses the runway at a distance of 1000 m from the runway threshold (see Figure 1). The runway crossing may be used for taxiing between the apron and a second runway, according to a runway crossing procedure that will be outlined later. The runway crossing has stopbars that are remotely controlled by the runway

controller. In the runway incursion scenario a taxiing aircraft is crossing the runway while it should not due to inappropriate situation awareness of its pilots.

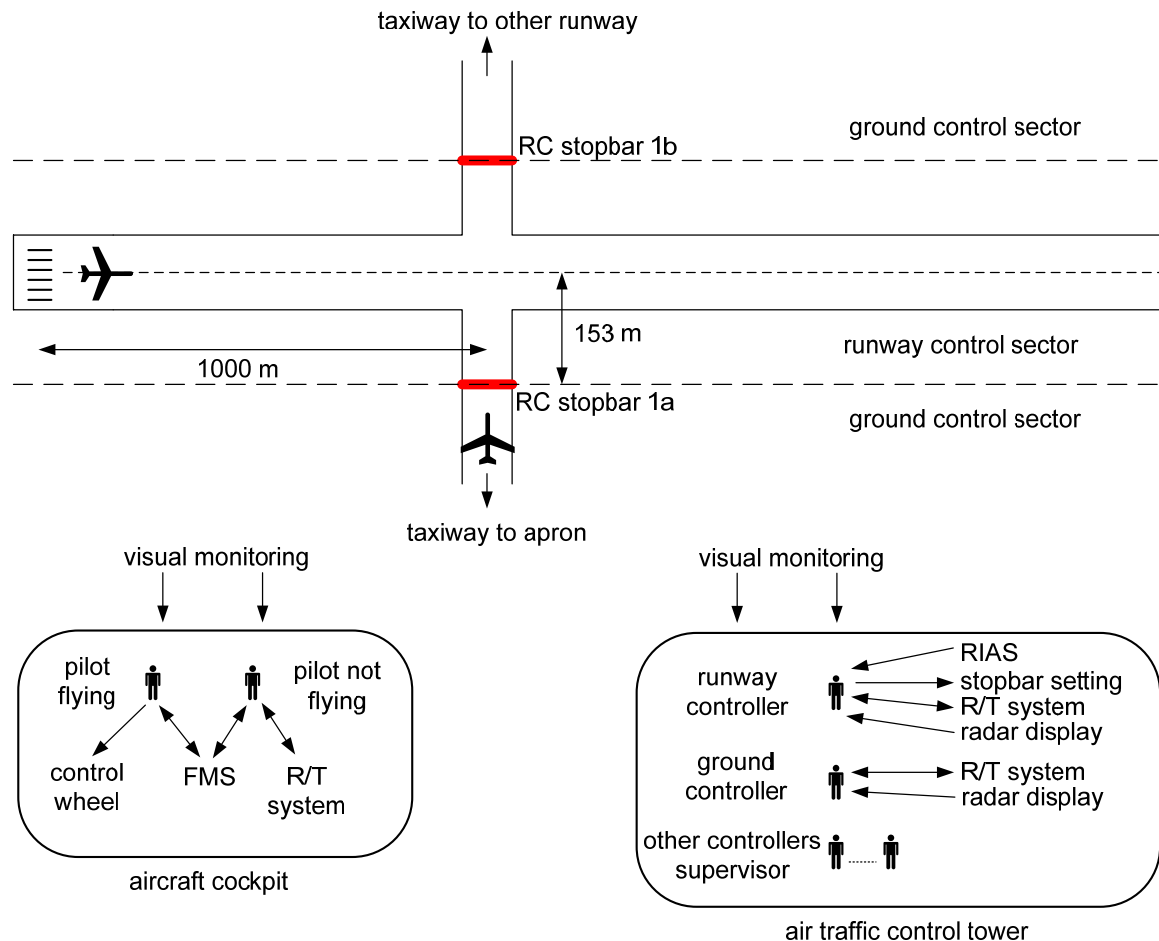


Figure 1: Schematic overview of the traffic situation considered. The taking-off aircraft accelerates along the runway while the crew of the taxiing aircraft intends to proceed along the taxiway towards the active runway. The various human operators and technical systems are discussed in the main text.

The operation is considered for weather conditions without wind and for two visibility conditions:

- *Visibility condition 1*: unrestricted visibility range; implying that pilots as well as controllers can visually observe the traffic situation. This is in line with visibility condition 1 of (ICAO, 2004).
- *Visibility condition 2*: visibility range between 400 m and 1500 m; implying that controllers cannot visually observe the traffic and pilots are not always able to see the conflicting aircraft during the initial part of the take-off run. The lower limit of this visibility range (400 m) is equal to the upper limit of

the runway visible range of visibility condition 3 indicated in (ICAO, 2004); the upper limit (1500 m) is chosen for this study (no value is given in (ICAO, 2004)).

The main human operators involved in the runway crossing operation are the pilots of the taking-off aircraft, the pilots of the taxiing aircraft, the runway controller and the ground controllers responsible for traffic on nearby taxiways. The pilots are responsible for safe conduct of the flight operations and should actively monitor for potential conflicting traffic situations. The runway controller is responsible for safe and efficient traffic handling on the runway and the runway crossings. The ground controllers are responsible for safe and efficient traffic handling on taxiways in the surroundings of the runway.

Aircraft may taxi across the active runway via the following procedure. The control over the taxiing aircraft is transferred from the responsible ground controller to the runway controller (including a change of the R/T frequency). Taking into consideration the traffic situation, the runway controller specifies a crossing clearance to the taxiing aircraft and switches off the remotely controlled stopbar. The crew of the taxiing aircraft acknowledges the clearance and initiates taxiing across the runway. After passage of the stopbar, it is automatically switched on again. The crew reports when the taxiing aircraft has vacated the runway, upon which the control over the aircraft is transferred from the runway controller to the responsible ground controller.

A runway incursion alert system (RIAS) may generate two types of alerts to warn the runway controller:

- Runway incursion alert for the situation that an aircraft is crossing the runway in front of an aircraft that has initiated to take off;
- Stopbar violation alert for the situation that an aircraft crosses an active stopbar in the direction of the runway.

These alerts consist of audible warnings and an indication on the ground surveillance display. The alerts are based on ground radar tracking data. The alert system is considered to have a high probability of detection and a low probability of a false alert.

Standard communication, navigation and surveillance systems are used:

- Communication between controllers and crews is by R/T systems;
- The pilots use their knowledge on the aerodrome layout and maps for taxiing;
- Ground radar tracking data of all aircraft and sufficiently large vehicles on the airport surface is shown on displays of the runway and ground controllers.

3 SAFETY RISK ASSESSMENT CYCLE

3.1 STEPS IN THE SAFETY RISK ASSESSMENT CYCLE

An overview of the steps in a TOPAZ safety risk assessment cycle is given in Figure 2. In step 0, the objective of the assessment is determined, as well as the safety context, the scope and the level of detail of the assessment. Step 1 serves to obtain a complete overview of the operation. Next, hazards associated with the operation are identified (step 2), and aggregated 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 main sources contributing to the lack of safety (safety bottlenecks) are identified (step 7). A more detailed discussion of the processes in these steps is provided in (Blom et al., 2006).

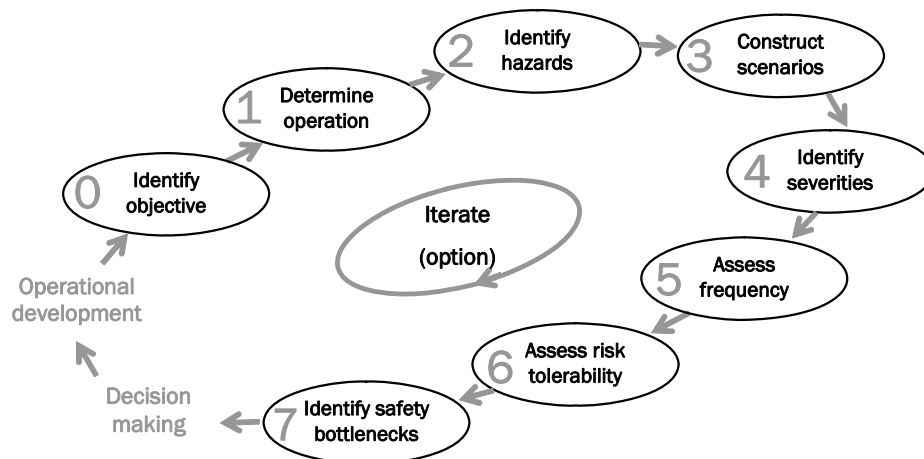


Figure 2: Steps in TOPAZ safety risk assessment cycle

The main results of the risk assessment cycle are the assessed risk levels and the identified safety bottlenecks. These results support decision making about the acceptability of the operation and identification of mitigating measures or improvements in the operation design. If the design is changed, a new safety risk assessment cycle of the operation should be performed in order to investigate how much the risk posed by previous safety issues has been decreased, but also

to assess any new safety issues that may have been introduced by the enhancements themselves.

Systemic accident modelling and Monte Carlo simulation play a key role in step 5, as will be discussed in Section 4 and following. To clarify the context of the Monte Carlo simulations, safety relevant scenario diagrams and the associated severity and frequency assessments are discussed next.

3.2 SAFETY RELEVANT SCENARIO DIAGRAM

A safety relevant scenario diagram is developed in step 3 on the basis of hazards identified in step 2. It represents relations between events/conditions that may lead to potentially hazardous air traffic situations and events/conditions that may hamper resolution of these air traffic situations. Figure 3 presents a generic safety relevant scenario diagram. In the context of the runway crossing operation, examples of the elements in Figure 3 are:

- Root hazard a: Pilots react on clearance for another aircraft and start crossing;
- Root hazard b: Pilots cross without clearance;
- Hazardous situation: Aircraft crossing runway while it should not;
- Condition: Other aircraft has initiated take-off;
- Conflict: Aircraft taking off while another aircraft is crossing the runway and it should not;
- Resolution hazard c: Pilots of crossing aircraft do not frequently look for conflicting traffic;
- Resolution hazard d: Pilots of crossing aircraft are not tuned to frequency of runway controller communication system;
- Conflict evolution: Possible ways of evolution of the runway incursion conflict, e.g. leading to some incident or an accident.

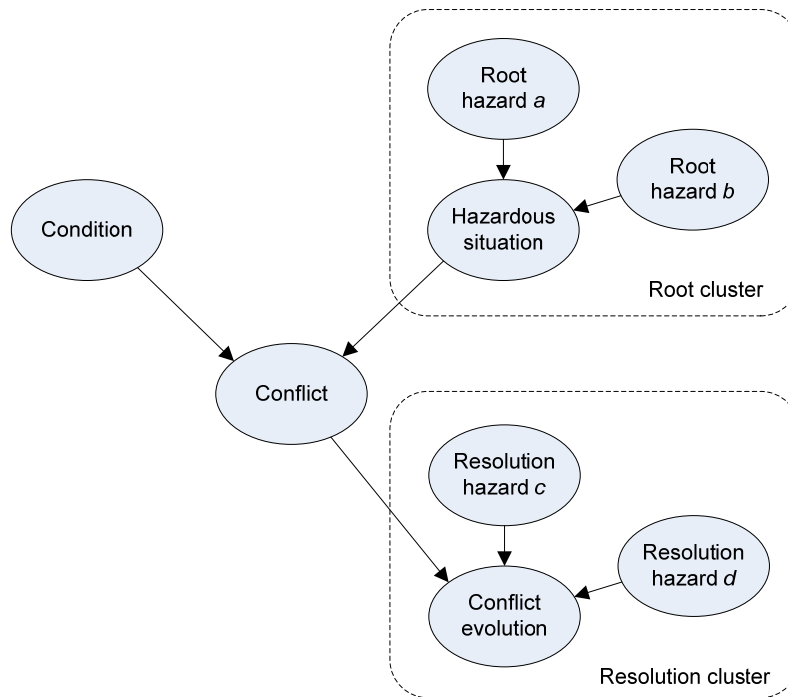


Figure 3: Generic safety relevant scenario diagram

By application of step 2 for the active runway crossing operation, the following safety relevant scenarios were identified (Blom et al. 2006):

- Scenario I: Aircraft erroneously in take-off and crossing aircraft on runway;
- Scenario II: Aircraft erroneously crossing and other aircraft in take-off;
- Scenario III: Aircraft taking off and runway unexpectedly occupied;
- Scenario IV: Aircraft crossing and runway unexpectedly occupied by aircraft;
- Scenario V: Aircraft crossing and vehicle on runway;
- Scenario VI: Collision between aircraft sliding off runway and aircraft near crossing;
- Scenario VII: Aircraft taking off and vehicle crossing;
- Scenario VIII: Jet-blast from one aircraft to another; and
- Scenario IX: Conflict between aircraft overrunning/climbing out low and aircraft using a nearby taxiway.

For our study of systemic accident assessment by Monte Carlo simulation we focus on scenario II in the sequel of this paper.

3.3 SEVERITY AND FREQUENCY ASSESSMENT

In step 4 of the safety risk assessment cycle, an evaluation is made of the range of severity categories that may apply to the possible ways of conflict evolution of

the safety relevant scenario. For instance, the severity of the outcome of a scenario may be considered 'serious incident' if the aircraft only avoid a collision at a short distance, or the severity category is 'accident' in case of a collision. The severity assessment does not address an evaluation of the probability of the severity; it simply assesses which severity categories may occur and which not, and it describes the associated characteristics of the conflict evolution. For scenario II, the most severe consequence is a collision between the two aircraft. To support risk assessment for the most severe consequences, the Monte Carlo simulations should thus support the assessment of the scenario up to the level of collision.

Next, in step 5, the occurrence frequency of the severity categories in the safety relevant scenario is assessed. In the Monte Carlo simulation based risk assessment of scenario II, we focus on the frequency of collisions between aircraft taxiing and taking-off. Referring to Figure 3, these Monte Carlo simulations represent the dynamic interactions of the agents in the initiation and evolution of the conflict between the two aircraft, given the hazardous situation that the taxiing aircraft is approaching the runway crossing while it should not. The Monte Carlo simulations thus provide the data for determination of conditional collision probabilities given the specific hazardous situations and contextual conditions. In a complete risk assessment also the probabilities of the hazardous situations (e.g. misconceptions, failures) and contextual conditions (e.g. visibility conditions) should be evaluated and combined with the conditional collision risks to obtain the overall accident risk of the scenario. In our risk assessments, primary sources of data for determination of such event probabilities are operational experts (e.g. pilots and controllers) and databases (e.g. aviation safety databases, local controller reporting systems).

The evolution of the conflict in the scenario may depend on a wide range of hazards and conditions. In particular, the specifics of the dynamic interactions between the agents in the Monte Carlo simulations may depend on the root hazards, the contextual conditions and the resolution hazards of the scenario. In this way, latent conditions that influence the performance of agents can be introduced. For instance, if the pilots of the taxiing aircraft believe to be proceeding on a normal taxiway, their visual monitoring performance differs from the situation when they know to be heading towards a runway crossing. An overview of the main interactions between the agents in the Monte Carlo simulation model of the runway crossing scenario is presented next.

4 MONTE CARLO SIMULATION MODEL

4.1 DEVELOPMENT OF A DYNAMIC STOCHASTIC MULTI-AGENT MODEL

The Monte Carlo simulations for safety analysis of air traffic scenarios are based on mathematical models, which uniquely define the stochastic dynamics of the related agents (human operators and technical systems). These models are specified by a compositional specification approach using a stochastic dynamic extension of the Petri net formalism (Everdij and Blom, 2006b). Within this Petri net formalism a hierarchically structured representation of the agents in the air traffic scenario is developed, including:

- Key aspects of the agents, e.g. situation awareness / task performance / task scheduling of a human operator, flight phases / performance modes of aircraft, or availability / status of an alert system;
- Modes within the key aspects of agents, e.g. task performance of a controller is monitoring / clearance specification / alert reaction, flight phase is taxiing / take-off run / rejected take-off / hold, or system availability is up / down;
- Dynamics within modes, e.g. the time needed for task performance, or the acceleration profile during take-off run, or the duration of an alert;
- Interactions between modes within key aspects, e.g. the transition to a next task, the transition to another flight phase, or a change in the availability of a system;
- Interactions between key aspects of an agent, e.g. the effect of situation awareness on task performance, the effect of an engine failure on a flight phase, or the effect of availability on the status of an alert;
- Interactions between agents, e.g. the effect of task performance of a pilot on the flight phase of an aircraft, or the effect of an alert on the situation awareness of a controller.

Here, the dynamics and interactions include deterministic and stochastic relationships, as is appropriate for the human performance or system considered.

4.2 OVERVIEW OF THE RUNWAY INCURSION MODEL

Figure 4 shows an overview of the interactions between the main agents of the runway incursion risk assessment model. A high-level description of the model is provided next.

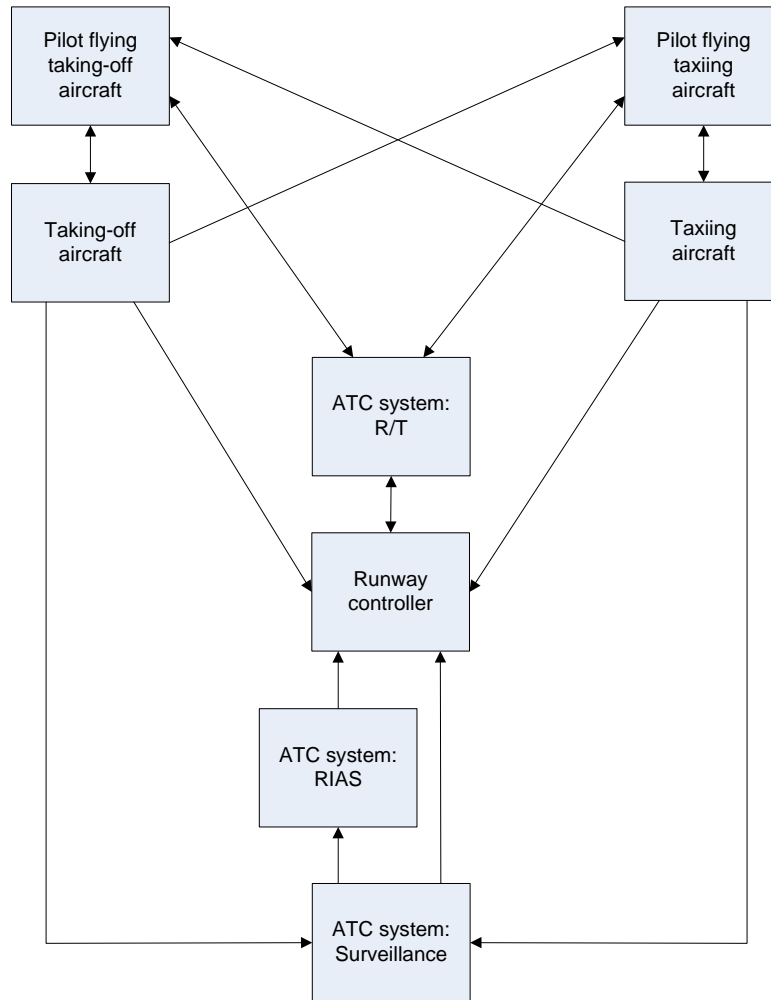


Figure 4: Interactions between the main agents of the runway incursion risk assessment model: aircraft, pilots flying, runway controller and ATC system (R/T, RIAS and surveillance)

VISIBILITY CONDITION

In the model, two visibility conditions are used:

- Visibility condition 1 with an unconstrained visibility range;
- Visibility condition 2 with a visibility range uniformly distributed between 400 m and 1500 m.

TAKING-OFF AIRCRAFT

The model of the taking-off aircraft represents the ground run, airborne transition and airborne climb-out phases during take-off and includes the possibility of a rejected take-off. The aircraft initiates take-off from a position near the runway threshold. The aircraft may have diminished acceleration or

deceleration power. Two types of aircraft are included in the model: medium-weight aircraft and heavy-weight aircraft.

TAXIING AIRCRAFT

The model of the taxiing aircraft represents aircraft movements (hold, acceleration, constant speed, deceleration) during taxiing. The taxiing aircraft enters the taxiway leading to the runway crossing at a position close to the remotely controlled stopbar (see Figure 1) with a normally distributed taxiing speed, or initiates taxiing from stance. The entrance time of the crossing aircraft is uniformly distributed around the take-off start time. The taxiing aircraft may have diminished deceleration power. Two types of aircraft are included in the model: medium-weight aircraft and heavy-weight aircraft.

SURVEILLANCE (ATC SUBSYSTEM)

The model of the surveillance system provides position and velocity estimates for both aircraft. There is a chance that the surveillance system is not available, resulting in track loss. Surveillance data is used by the ATC runway incursion alert system. In visibility condition 2, surveillance data is used for monitoring by the runway controller.

RIAS (ATC SUBSYSTEM)

The model of the runway incursion alert system includes two types of alerts:

- A stopbar violation alert is presented to the controller if surveillance data indicates that an aircraft has passed an active stopbar. There is a chance that the stopbar violation alert is not functioning.
- A runway incursion alert is presented to the controller if surveillance data indicates that the taxiing aircraft is within a critical distance of the runway centre-line and the taking-off aircraft has exceeded a velocity threshold in front of the runway crossing. There is a chance that the runway incursion alert is not functioning.

R/T (ATC SUBSYSTEM)

The model for the R/T system between the runway controller and the aircraft crews accounts for the communication system of the aircraft, the communication system of the controller, the tower communication system and the frequency

selection of the aircraft communication system. The nominal status of these communication systems accounts for direct non-delaying communication. The model accounts for the chance of delay or failure of the communication systems.

PILOT FLYING OF TAKING-OFF AIRCRAFT

The model for the performance of the pilot flying (PF) of the taking-off aircraft accounts for performance of tasks such as auditory monitoring, visual monitoring, crew coordination, aircraft control, and conflict detection and reaction. The model includes dynamic representations of the situation awareness of the pilot, the cognitive control mode of the pilot and task scheduling by the pilot.

Initially, the PF of the taking-off aircraft is aware that take-off is allowed and initiates a take-off. During the take-off the PF visually monitors the traffic situation on the runway. During a monitoring action the PF may not observe the intruding taxiing aircraft, primarily because the distance with the crossing aircraft exceeds a maximum viewing distance set by the visibility condition. The PF of the taking-off aircraft may detect a conflict with a taxiing aircraft,

- if the taxiing aircraft is observed to be within a critical distance of the runway, or
- due to an R/T call of a controller. A controller call may, however, not be properly understood by the PF.

Following conflict detection, the PF starts a collision avoiding braking action if it is expected that braking will stop the aircraft in front of the taxiing aircraft.

PILOT FLYING OF TAXIING AIRCRAFT

The model structure for the PF of the taxiing aircraft is similar to that of PF of the taking-off aircraft. Initially, the PF of the taxiing aircraft may intend to continue taxiing on a regular taxiway (not crossing a runway) or to cross the active runway. Note that in both cases the situation awareness of the PF is not correct. During taxiing the PF visually monitors the traffic situation. If the PF is aware to be approaching the runway crossing, visual monitoring is done more frequently than in the case that the PF is aware to be on a regular taxiway. The PF may detect a conflict with the taking-off aircraft,

- if the taxiing aircraft is within a critical distance of the runway, the taking-off aircraft approaches the taxiing aircraft and the speed of the taking-off aircraft exceeds a threshold value, or

- due to an R/T call of a controller. A controller call may, however, not be properly understood by the PF.

Following conflict detection, the PF starts a collision avoiding braking action unless the taxiing aircraft already is within a critical distance of the runway centre-line.

RUNWAY CONTROLLER

The model for the performance of the runway controller accounts for performance of tasks such as visual monitoring, communication with aircraft crews, ATC coordination, and conflict detection and reaction. The model includes dynamic representations of the situation awareness of the controller, the cognitive control mode of the controller and task scheduling by the controller.

The runway controller monitors the traffic situation on the runway and is supported by stopbar violation alerting and runway incursion alerting systems. Monitoring is done visually in visibility condition 1 and is done via ATC surveillance data in visibility condition 2. The situation awareness updating times as a result of monitoring depend on other controller tasks, such as co-ordination with other controllers and complementary communication with aircraft crews.

The controller may detect a safety-critical situation,

- if the controller observes that the taxiing aircraft has passed the stopbar, or
- due to a stopbar violation alert, or
- due to a runway incursion alert.

Following detection of the safety-critical situation, the controller instructs both the taxiing aircraft and the taking-off aircraft to hold.

4.3 PARAMETERISATION OF THE SIMULATION MODEL

Once the mathematical structure of the simulation model has been specified (agents, key aspects, modes, dynamics and all interactions), appropriate parameter values should be chosen that represent the operation considered. Parameter values are based on a variety of sources, such as

- technical system specifications, e.g. requirement on availability of alert system;
- scientific expertise and literature on safety and human factors, e.g. task performance;
- searches in incident databases, e.g. frequency of specific runway incursions;
- interviews with operational experts, e.g. scanning patterns by pilot;

- measurement data from real operations, e.g. taxiing speeds;
- measurement data from real-time simulations, e.g. controller performance aspects;
- simulation results from other relevant models, e.g. Air-MIDAS human performance modelling (Corker, 2000; Blom et al., 2005).

In practice, limited data on appropriate parameter values is available for the contextual conditions considered, leading to a credibility interval of possible parameter values. Typically, the mean of this interval is chosen for the simulation model and an analysis of the effect of the uncertainty in the parameter value on the risk is included in a bias and uncertainty assessment (see Section 6). If the uncertainty in the parameter value has a significant effect on the risk, an additional effort may be done to attain a better estimate.

4.4 SPEED-UP OF MONTE CARLO SIMULATION

Air traffic is a very safe means of transport. Consequently, the risk of collision between two aircraft is extremely low. The assessment of such low collision risk values through straightforward Monte Carlo simulation would need extremely lengthy computer simulation periods. Therefore, speed-up of Monte Carlo simulations is required, which may be achieved by risk decomposition. This consists of decomposing accident risk simulations in a sequence of conditional Monte Carlo simulations and combining the results of these conditional simulations into the assessed collision risk value. To this end, we use stochastic analysis tools to model and analyse in a proper way the arbitrary stochastic event sequences (including dependent events) and the conditional probabilities of such event sequences in stochastic dynamic processes (Blom et al., 2003).

For the active runway crossing example, the particular conditions taken into account for this risk decomposition are:

- (a) Type of each aircraft (medium-weight or heavy-weight);
- (b) Remotely controlled stopbar (functioning or not);
- (c) Communication systems (functioning or not);
- (d) RIAS (functioning or not);
- (e) Situation awareness (SA) of the PF of the taxiing aircraft concerning allowance of runway crossing (allowed / not allowed);
- (f) SA of the PF of the taxiing aircraft concerning the next way-point (taxiway/crossing);
- (g) Visibility condition (1 or 2).

For the results presented in this paper, event probabilities of conditions (a) to (e) are included in the Monte Carlo simulations. Conditional collision risks are assessed given (f) and (g), i.e. given the two options for the SA of the PF of the taxiing aircraft and given the two options for the visibility condition (resulting in four combined options).

Based on the simulation model and the accident risk decomposition, Monte Carlo simulation software is developed to evaluate the event probabilities and the conditional collision risks, and to compose the collision risk assessed by the simulation model. In the remainder of this paper conditional collision risks are estimated given conditions (f) and (g). Results for total collision risks, obtained by combining conditional risks with the probabilities of the conditions, are provided in (Stroeve et al., 2003) and (Blom et al., 2006) for visibility condition 1.

5 MONTE CARLO SIMULATION OF RUNWAY INCURSION

Point estimates of the conditional collision risks achieved in the Monte Carlo simulations on the basis of the model and software described in Section 4 are shown in Figure 5 for the cases with and without the runway incursion alert system. The collision risks are conditional on the visibility condition and the situation awareness of the pilot flying of the taxiing aircraft, which represents the intention to either continue taxiing on the current regular taxiway or to cross the runway.

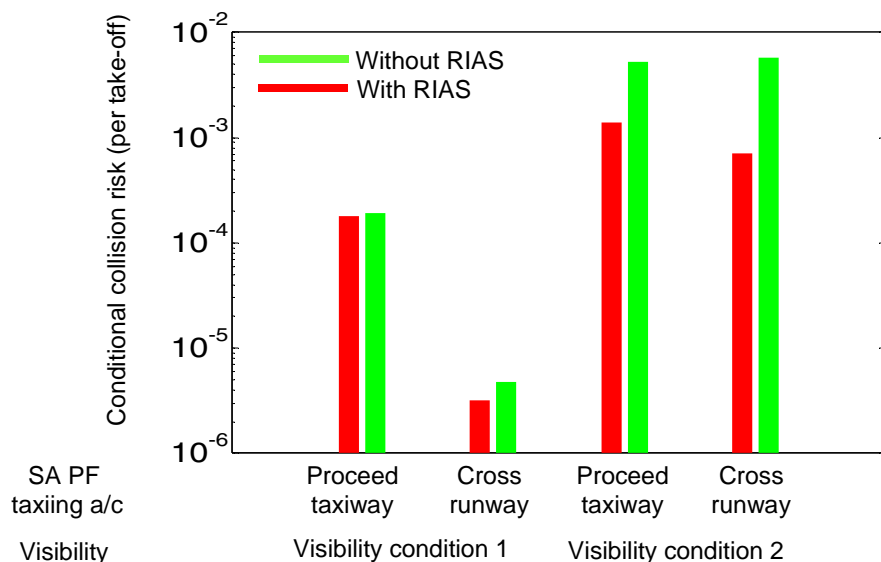


Figure 5: Monte Carlo simulation results for conditional collision risk given situation awareness of pilot flying of taxiing aircraft (Proceed taxiway / Cross runway) and visibility condition (1 / 2) for the cases without and with RIAS

The Monte Carlo simulation results in Figure 5 show that for an unrestricted visibility range (visibility condition 1) the conditional collision risk strongly depends on the situation awareness of the pilot flying of the taxiing aircraft. This difference is mainly caused by the improved (more frequent) monitoring strategy in the model for the case that the pilot intends to cross the runway compared to the case that the pilot intends to proceed on a regular taxiway. The Monte Carlo simulation results show that the effectiveness of the ATC alerts in visibility condition 1 is very small. In this situation the conflict has almost always been

recognised by the pilots of one or both aircraft before the controller has the chance to react to the alert and instruct the pilots, and in the remaining cases the controller can usually not timely warn the pilots.

For a visibility range between 400 m and 1500 m (visibility condition 2), the Monte Carlo simulation-based risks are quite different. Firstly, it can be observed in Figure 5 that similar conditional collision risks are obtained for both the cases of situation awareness of the pilot flying of the taxiing aircraft. In this visibility condition, the improved monitoring strategy of the pilot does not support early-stage recognition of the conflict. Secondly, in this visibility condition the ATC alerts enable a significant reduction in the conditional collision risk. Here, the conflict can often not be recognised by the pilots at an early stage and the alerts reduce the conflict detection time for the controller. The larger effectiveness of the alerts for the case where the pilot is intending to cross the runway can be explained by the model aspect that in this case the aircraft may initiate taxiing from stance, thereby increasing the time before it reaches the collision critical zone on the runway.

6 BIAS AND UNCERTAINTY ASSESSMENT

6.1 VALIDATION: ASSESSMENT OF DIFFERENCES BETWEEN MODEL AND REALITY

By definition, any model differs from reality. Hence, validation of a model is supported by identification of these differences and evaluation of their impact at the assessed risk level in terms of bias and uncertainty:

- Bias: the model-based accident risk is systematically higher or lower than the risk of the real operation;
- Uncertainty: the model-based accident risk lies in a range of credible values for the risk of the real operation (e.g. a 95% credibility interval).

As an integrated part of the accident risk assessment methodology TOPAZ, a bias and uncertainty assessment method has been developed (Everdij et al., 2006a). This method supports identification of differences between the Monte Carlo simulation model and reality, and subsequent evaluation of the bias and uncertainty due to these differences (see Figure 6). The Monte Carlo simulations provide risk point estimates and risk sensitivities that are used in the bias and uncertainty assessment to obtain an extended insight in the risk of the real operation.

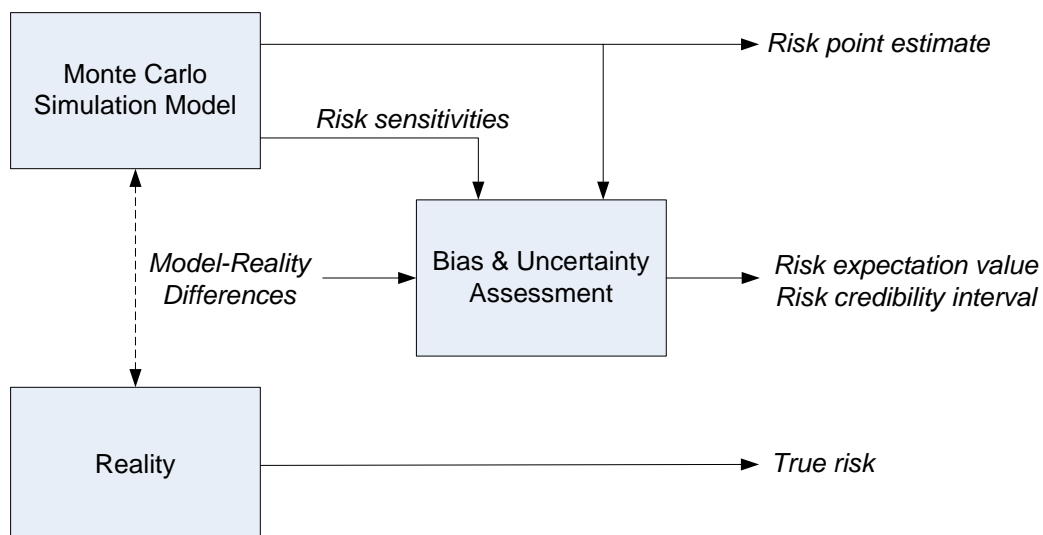


Figure 6: The Monte Carlo simulations play a dual role in the risk assessment by providing a risk point estimate and risk sensitivities, which are both used in the bias and uncertainty assessment

6.2 STEPS IN THE BIAS AND UNCERTAINTY ASSESSMENT

The bias and uncertainty assessment method consists of the following steps:

1. Identify all potential differences between the simulation model and reality;
2. Assess the size/probability of each difference;
3. Assess the sensitivity of simulation results for changes in parameter values;
4. Assess the effect of each difference on the risk outcome;
5. Determine the joint effects of all differences.

A concise introduction of these steps is provided next; more details and mathematical background is given in (Everdij et al., 2006a).

STEP 1: IDENTIFY ALL POTENTIAL DIFFERENCES BETWEEN THE SIMULATION MODEL AND REALITY

During the development of a Monte Carlo simulation model and at the start of a bias and uncertainty assessment of the simulation results of a particular operation, a broad list of potential differences between model and reality is identified. No assessment of the effects of these differences is done yet, such that seemingly unimportant differences are also included. In support of this step, five types of differences are distinguished:

- *Numerical approximations*: numerical approximations used for the accident risk evaluation of the model, e.g. the integration method used for evaluation of differential equations;
- *Parameter values*: uncertainty/bias in the choice of values of the model parameters, e.g. the average velocity during taxiing;
- *Formal model structure*: the model structure does not completely describe the air traffic scenario in all detail, e.g. conflict recognition by the ground controller is not included in the Monte Carlo simulation model;
- *Non-covered hazards*: hazards of the operation that are not incorporated by the model, e.g. a hazard like 'Aircraft in take-off has problems and runs into aircraft close to a crossing point' is not represented in the Monte Carlo simulation model; the take-off run follows the runway centre-line;
- *Operational concept differences*: differences between the operational concept for which the accident risk model was developed and the operational concept for which the accident risk is assessed, e.g. assessment of a 'crossing behind take-off'-procedure by a model without such dependent crossing procedures.

STEP 2: ASSESS THE SIZE/PROBABILITY OF EACH DIFFERENCE

For each difference it is assessed how large it is, or how often it may happen. In particular, for each parameter value the size of a 95% credibility interval and a bias factor are assessed. For each other type of difference, a value is assessed for the probability that the difference exists in the case considered. In support of this step, categories are defined of the sizes of bias factors and credibility intervals (e.g. Negligible, Small, Minor, Significant, Considerable, Major) and of the probabilities of differences (e.g. Unlikely, Infrequent, Frequent, Typical).

STEP 3: ASSESS THE SENSITIVITY OF SIMULATION RESULTS FOR CHANGES IN PARAMETER VALUES

The normalized sensitivities of the risk outcomes of the simulation model for changes in the parameter values are assessed. Typically, a model expert performs a first assessment of sensitivity categories (e.g. Negligible, Small, Minor, etc.) by using knowledge of the simulation model. Next, parameter values with sensitivities and risk effects that have been preliminary assessed to be more than Negligible are assessed using additional Monte Carlo simulations (for the assessment of risk effects feedback from step 4 is used).

STEP 4: ASSESS THE EFFECT OF EACH DIFFERENCE ON THE RISK OUTCOME

The bias and credibility interval of each parameter value are combined with the risk sensitivity to find the bias and credibility interval in the risk for the parameter value considered. For each other (non-parameter value) difference, a conditional risk bias given the difference exists, is assessed. This assessment uses feedback from operational experts and the insights gained from the sensitivity study in step 3. The probability that the difference exists and the conditional risk bias are combined to a risk bias for each difference.

STEP 5: DETERMINE THE JOINT EFFECTS OF ALL DIFFERENCES

All assessment results of the risk effects of the differences identified between the Monte Carlo simulation model and reality are combined to find a bias and 95% credibility interval of the risk (Everdij et al., 2006a). With this the expected value and 95% credibility interval of the risk of the scenario are achieved.

6.3 BIAS AND UNCERTAINTY RESULTS FOR THE RUNWAY INCURSION SCENARIO

The above described bias and uncertainty assessment steps have been performed for the runway incursion scenario in which the pilot flying (erroneously) thinks to proceed on a normal taxiway, in visibility condition 1 and with ATC supported by a runway incursion alert system. First, safety experts identified differences between the Monte Carlo simulation model and reality. In total, 306 differences between model and reality have been identified, consisting of 175 parameter values and 131 other differences. Subsequently, safety experts made a first selection of the most important differences, i.e. the differences with non-negligible effects on the collision risk.

For these most important differences, the opinions of two pilots and two controllers were obtained via structured interviews, which addressed about 25 topics. Table 1 shows examples of the kinds of questions for the operational experts. It can be observed that these questions are quite different from expert interviews for sequential and epidemiological accident models. There, the data required usually are event probabilities, often conditional on the contextual situation, e.g. the probability of a human operator not detecting an abnormal situation. Here, the kinds of data are more diverse, reflecting a wide range of performance data for human operators and technical systems.

Table 1: Examples of questions for controllers and pilots during interviews for bias and uncertainty assessment

Examples of controller questions
If the runway controller has recognised a runway incursion conflict, how long would it take to instruct the intruding aircraft?
If the intruding aircraft is not on the frequency of the runway controller, how long would it take to reach it via coordination with a ground controller?
In which situations would the runway controller first try to stop the aircraft taking-off rather than the aircraft taxiing?
Examples of pilot questions
How much time is required to initiate a rejected take-off after an instruction by ATC?
In what situations does the PF of an aircraft taking off consider a taxiing aircraft as conflicting, for instance, position / speed of taxiing aircraft?
What is the angular range for visual monitoring by the pilot flying during taxiing?
How often does the pilot look outside during taxiing to visually monitor the traffic situation?

The opinions of the pilots and controllers as well as the results of additional Monte Carlo simulations were used by the safety experts to evaluate the effect of

the differences on the risk. The combined effect of the identified differences on the bias and uncertainty in the conditional collision risk for the situation considered is shown in Figure 7. There is a small bias, indicating that the Monte Carlo simulation-based risk is somewhat conservative, and a 95% credibility interval with a range of a factor 6 above to a factor 30 below the expected risk level.

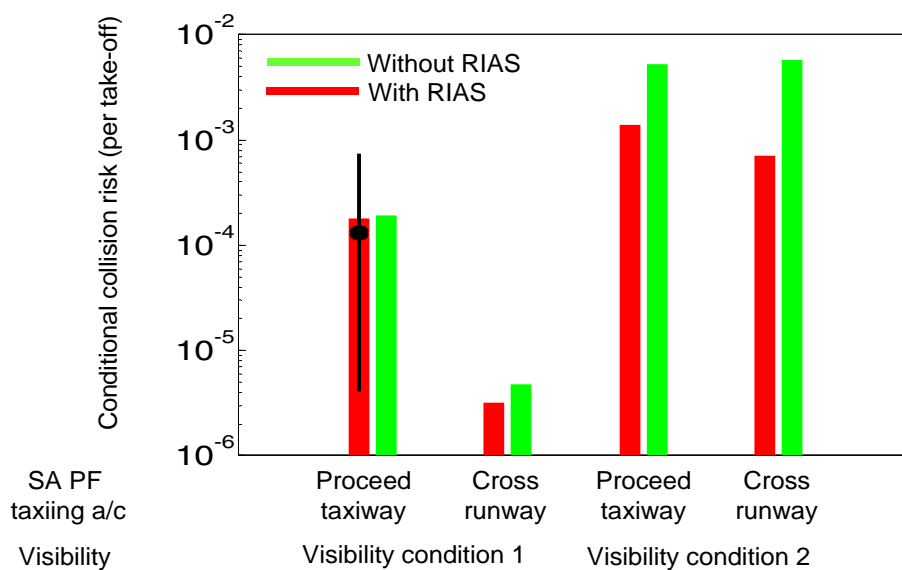


Figure 7: Monte Carlo simulation results of Figure 5 plus the results of the bias and uncertainty assessment for the case selected. The narrow bar represents the 95% credibility interval and the dot represents the expected value of the collision risk.

In addition to an estimate of the expected risk and its credibility interval, the bias and uncertainty assessment gives information on the size of the effect on the risk of each difference and provides feedback on the aspects of the operation that mostly contribute to the risk. Table 2 provides a list of the differences between the Monte Carlo simulation model and reality with more than 30% effect on the bias and/or size of the credibility interval of the assessed conditional collision risk level in the runway incursion scenario considered. These differences all relate to pilot and aircraft performance. Table 3 gives examples of differences with less than 13% effect (95% of the differences belong to this class). It follows that the ATC runway incursion alert system has little effect on the assessed risk level for the situation considered.

Table 2: List of differences between model and reality with more than 30% effect on the bias and/or uncertainty for the selected case of the runway incursion scenario

Differences with more than 30% effect on bias or uncertainty
The types of manoeuvres of the taking-off aircraft that can be performed to avoid a collision (only braking or also other manoeuvres, e.g. lateral movement)
The contribution of the pilot not flying of the taxiing aircraft to prevention of a collision
Deciding by the pilots of the taking-off or taxiing aircraft if an other aircraft is considered to be conflicting
The speed of the taxiing aircraft
The monitoring frequency by the pilot of the taxiing aircraft
The deceleration of taking-off and taxiing aircraft in case of braking to avoid a collision
The time before braking is initiated by the pilots of the taking-off aircraft

Table 3: Examples of differences between model and reality with less than 13% effect on the bias and/or uncertainty for the selected case of the runway incursion scenario

Examples of differences with less than 13% effect on bias or uncertainty
Variation in the take-off weight of the aircraft
Variation in the take-off thrust of the aircraft
The lift-off velocity of the aircraft
The acceleration profile during the take-off run
The aircraft manoeuvre during the airborne transition phase
The take-off performance during engine failure
The performance of the VHF R/T communication systems
The performance of the surveillance tracking systems
The performance of the runway incursion alert system
The task scheduling of the runway controller

6.4 POTENTIAL IMPLICATIONS OF THE RISK ASSESSMENT RESULTS

The expected risk and its credibility interval support the decision making process regarding the acceptability of the assessed risk, the acceptability of the uncertainty in the assessed risk and potential further design of the operation considered. If the uncertainty in the assessed risk is high and this implies that the required target level of safety may not be attained, a reduction of the uncertainty may be strived for. This may be achieved by obtaining more information on the operation and the accident scenario considered, such as additional data from real operations, real-time simulations or other relevant Monte Carlo simulations, additional interviews with operational experts, and additional searches in incident databases. This additional information can then be used to update the simulation model, such that the effects of differences between model and reality are reduced. The choice for the uncertainty reducing approaches depends on the available means, and is supported by bias and

uncertainty assessment results for the most important risk determining differences between the simulation model and reality.

The sensitivity analysis within the bias and uncertainty assessment supports the identification of aspects of the operation that lead to potential exceeding of target levels of safety ('safety bottlenecks'). Such safety bottlenecks support identification of mitigating measures and redevelopment of the operation. For instance, if the taxiing speed at particular airport locations seems a safety bottleneck, it may be decided to implement speed restrictions.

On the other hand, the sensitivity analysis provides insight in aspects of the operation that are less important for its risk. For such aspects, relatively mild safety requirements may be formulated that can be implemented cost effectively. For instance, the requirements for the availability of a runway incursion alert system may be less stringent if the effect of such an alert on the collision risk is small.

7 DISCUSSION

A systemic accident model considers accidents as emergent phenomena from variability and interactions in a complex system (Hollnagel, 2004). Air traffic risk assessments have predominantly been done by sequential and epidemiological accident models. In this paper, we have demonstrated the feasibility of a practical risk assessment of a runway incursion scenario by a systemic approach and showed the unique results that can thus be attained. This systemic approach is based on the TOPAZ methodology and uses Monte Carlo simulations of dynamic interactions of relevant agents to analyse safety-relevant scenario. Next, we discuss key aspects of systemic accident modelling and their relation with the methods and results presented in this paper.

A key aspect of systemic accident models is the emergence of accidents due to interactions in a complex organization. In the Monte Carlo simulations of the runway incursion scenario, accidents may emerge from an unfortunate combination in the variability of the performance of the interacting agents, for example, an aircraft has just started the take-off run, another aircraft is taxiing towards the runway without its pilots knowing their position, the pilot flying of the aircraft taking-off does not recognize the conflict in time to stop the aircraft before the crossing position, the pilot flying of the aircraft taxiing has not noticed the conflict, and the runway controller is alerted but can only communicate with the pilots at a stage where they are not able to resolve the conflict. In our systemic model, such chains of events are not pre-programmed, but they may emerge from the agents' interactions and performance variability. Even the events themselves are often not defined a priori but emerge, for example, visual monitoring times and thereby conflict recognition times by the pilots are variable and the event that the pilots recognize the conflict in time to prevent an accident emerges from the Monte Carlo simulations. Here, events like 'recognize the conflict in time' can only be classified after the scenario has been simulated for a specific case; the same visual monitoring interval may be too late in some cases and in time in other cases, depending on other agents' aspects like, e.g. the taxiing speed or braking deceleration. In contrast with the emergence of safety occurrences in the Monte Carlo simulations, in sequential accident models as fault and event trees, events and the ordering of events are defined by the safety analyst. To be able to manage the complexity of such sequential models, it is usually needed to restrict the number of events and the

ways in which they are ordered and interact. Doing so, critical interdependencies may be neglected in a risk assessment based on a sequential accident model.

A systemic accident model endeavours to describe the performance of a system or operation as a whole. In line with such a wide scope endeavour, the risk assessment of the runway incursion scenario presented in this paper considers the dynamic interactions between a wide range of human operators and technical systems: multiple aircraft, their pilots flying, runway controller, surveillance system, communication system and alert system. Moreover, the performance of these agents is described for a variety of nominal and non-nominal conditions, such as situation awareness differences and technical failures. This broad scope is required to obtain meaningful accident risk results in the systemic approach. In particular, as accidents in air traffic involve aircraft, which are directly controlled by pilots, a systemic accident model for air traffic cannot do without models for aircraft and pilot performance. In contrast, in risk assessments using sequential accident models it is not unusual to restrict the scope to a (new) technical system and its direct relations with other technical systems and human operators. For instance, in a related safety case on advanced surface movement guidance and control systems (Eurocontrol, 2006), the scope is focused on these systems, which allowed to use a sequential accident risk approach.

In line with the broad scope of our systemic accident model, the risk values that emerge from the Monte Carlo simulations are based on a broad scope of models of the various agents. These models describe variability in the performance of technical systems (e.g. aircraft performance during take-off, radar performance), human operators (e.g. visual observation, situation awareness) in varying contextual conditions (e.g. crossing position, visibility condition). Development and use of these models requires a broad knowledge base and a large variety of data sources (e.g. aircraft performance data, alert system settings, technical failure data, human task durations, etc.). In contrast, in sequential accident models like fault and event trees, accident occurrence is based on combining events via logical operators and obtaining risk values via event probabilities. Thus the kind of knowledge required is considerably different for systemic and sequential accident models.

In safety-relevant scenarios involving interactions between multiple dynamic agents (as customary in air traffic), the dependencies between risk contributions of agents are of special interest. In the presented systemic accident model, these risk dependencies emerge from concurrently interacting agents in the simulations, for example, observation by a pilot of moving aircraft, or

communication between pilot and controller. In a sequential accident model, conditional event probabilities must be specified by the safety analyst to cope with the dependent dynamics of interacting agents. For instance, the kind of data that might be required in such modelling is 'the probability that an alerted controller warns the pilots if the taxiing aircraft is at position X and given that the crews of the taxiing aircraft as well as the taking-off aircraft have not yet detected the conflict.' Since it is usually difficult to obtain such conditional probabilities, one typically has to assume that events happen independently from each other in applying sequential accident models.

The particular results that emerge from the Monte Carlo simulations of the considered runway incursion scenario are that in good visibility conditions the runway incursion alert system is not an effective means to reduce the conditional collision risk. This is not due to poor performance of the modelled runway incursion alert system as such: with high probability it provides an alert if the considered alert threshold settings are exceeded. However, in good visibility conditions, one or both cockpit crews usually have detected the conflict before they are warned by the alerted controller, and in the remaining cases the controller can usually not timely warn the pilots. In reduced visibility conditions (visibility in the range of 400 to 1500 m), the Monte Carlo simulations show that the same runway incursion alert system effectively reduces the conditional collision risk. In this case, the chance that the pilots have recognized the conflict themselves before they are warned by the alerted controller is reduced. These different types of results emerge from the systemic accident model basically via a difference in the modelled observation distance of the pilots. In contrast, to obtain such results by a sequential accident model, one would have the difficult job to assess separate event probabilities for the visibility conditions considered.

A validation process of the systemic accident model has been presented that is based on assessment of risk effects of (potential) differences between model and reality. This assessment is supported by Monte Carlo simulations that provide risk point estimates and risk sensitivities for parameter value changes. Since the parameter values usually refer to well interpretable processes, the risk sensitivity analysis provides added insight in the risk contributions of operational aspects in the safety relevant scenario considered. For the runway incursion scenario with the particular case that the pilot flying (erroneously) thinks to proceed on a normal taxiway in visibility condition 1, the validation process results indicate a small risk bias and a sizeable 95% credibility interval. The largest effects on bias and uncertainty in this case are due to pilots' performance; the effects on bias

and uncertainty due to controller performance and ATC systems are negligible. It means that a reduction in the risk uncertainty in this situation must come from better knowledge and data of pilots' performance.

In conclusion, we have shown that Monte Carlo simulation of safety relevant air traffic scenarios, such as used in TOPAZ, is a viable way of systemic accident assessment, and we have demonstrated the risk and validation results attainable by such modelling for a particular runway incursion scenario. The presented approaches can be effectively used to support particular safety cases for aerodrome operations.

ACKNOWLEDGEMENTS

We would like to thank two anonymous reviewers and Mariken Everdij (NLR) for their valuable comments on the paper.

8 REFERENCES

- Ale BJM, Bellamy LJ, Cooke RM, Goossens LHJ, Hale AR, Roelen ALC, Smith E (2006). Towards a causal model for air transport safety - an ongoing research project. *Safety Science* 44(8):657-673
- Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB (2001a). Accident risk assessment for advanced air traffic management. In: Donohue GL and Zellweger AG (eds.), *Air Transportation Systems Engineering*, AIAA, pp. 463-480
- Blom HAP, Daams J, Nijhuis HB (2001b). Human cognition modelling in air traffic management safety assessment. In: Donohue GL and Zellweger AG (eds.), *Air Transportation Systems Engineering*, AIAA, pp. 481-511
- Blom HAP, Bakker GJ, Everdij MHC, Van der Park MNJ (2003). Collision risk modelling of air traffic. In: Maciejowski JM (ed.), *Proceedings IFAC European Control Conference 2003 (ECC03)*, Cambridge, UK
- Blom HAP, Corker KM, Stroeve SH (2005). Study on the integration of human performance and accident risk assessment models: Air-MIDAS & TOPAZ. 6th USA/Europe ATM R&D Seminar, Baltimore, USA
- Blom HAP, Stroeve SH, De Jong HH (2006). Safety risk assessment by Monte Carlo simulation of complex safety critical operations. In: Redmill F, Anderson T (eds.), *Developments in risk-based approaches to safety*, Springer-Verlag, London, pp. 47-67
- Corker K (2000). Cognitive models & control: Human & system dynamics in advanced airspace operations. In Sarter N, Amalberti R (eds.), *Cognitive engineering in the aviation domain*, Lawrence Earlbaum Associates, New Jersey
- EUROCAE (2000). ED78A Guidelines for approval of the provision and use of ATS supported by data communication
- Eurocontrol (2004a). Air navigation system safety assessment methodology. SAF.ET1.ST03.1000-MAN-01, edition 2.0
- Eurocontrol (2004b). European action plan for the prevention of runway incursions, release 1.1
- Eurocontrol (2006). A-SMGCS Levels 1 and 2 Preliminary Safety Case. Edition 2.0
- Everdij MHC, Blom HAP (2002). Bias and uncertainty in accident risk assessment. National Aerospace Laboratory NLR, report NLR-CR-2002-137
- Everdij MHC, Blom HAP, Stroeve SH (2006a). Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. In: Stamatelatos MG, Blackman HS (eds.), *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*, May 14-18 2006, New Orleans, USA

- Everdij MHC, Klompstra MB, Blom HAP, Klein Obbink B (2006b). Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets. In: Blom HAP, Lygeros J (eds.), *Stochastic Hybrid Systems: Theory and safety critical applications*, LNCIS 337, Springer, pp. 325-350
- Greenberg R, Cook SC, Harris D (2005). A civil aviation safety assessment model using a Bayesian belief network (BNN). *The Aeronautical Journal*, November 2005, pp. 557-568
- Hollnagel E (2004). *Barriers and accident prevention*. Ashgate, Hampshire, England
- Hollnagel E, Woods DD (2005). *Joint cognitive systems: Foundations of cognitive systems engineering*. CRC Press, Boca Raton (FL), USA
- ICAO (2004). *Advanced Surface Movement Guidance and Control System (A-SMGCS) Manual*. Doc 9830, AN/452, first edition
- Kardes E, Luxhoj JT (2005). A hierarchical probabilistic approach for risk assessments of an aviation safety product folio. *Air Traffic Control Quarterly* 13(3):279-308
- Lee SM, Pritchett AR, Corker KM (2007). Evaluating transformations of the air transportation system through agent-based modeling and simulation. 7th USA/Europe ATM R&D Seminar, Barcelona, Spain
- Pariès J (2006). Complexity, emergence, resilience... In: Hollnagel E, Woods DD, Leveson N (eds.). *Resilience engineering: Concepts and precepts*. Ashgate, Aldershot, England
- Perrow C (1984). *Normal accidents: Living with high risk technologies*. Basic Books, New York, USA
- Reason J (1997). *Managing the risk of organizational accidents*. Ashgate, Aldershot, England
- Shah AP, Pritchett AR, Feigh KM, Kalaver SA, Jadhav A, Corker KM, Holl DM, Bea RC (2005). Analyzing air traffic management systems using agent-based modelling and simulation. 6th USA/Europe ATM R&D Seminar, Baltimore, USA
- Sträter O (2005). *Cognition and safety: An integrated approach to system design and assessment*. Ashgate, Hampshire, England
- Stroeve SH, Blom HAP, Van der Park MNJ (2003). Multi-agent situation awareness error evolution in accident risk modelling. 5th USA/Europe ATM R&D Seminar, Budapest, Hungary
- Stroeve SH, Blom HAP, Bakker GJ. Safety risk impact analysis of an ATC runway incursion alert system. Eurocontrol Safety R&D Seminar, Barcelona, Spain, 25-27 October 2006
- Wiegmann DA, Shappel SA (2001). Human error analysis of aviation accidents: Application of the Human Factors Analysis and Classification System (HFACS). *Aviation, Space, and Environmental Medicine* 72(11):1006-1016