NLR Air Transport Safety Institute

Research & Consultancy

NLR-TP-2013-489

SAFETY ASSESSMENT OF A FUTURE TAXI INTO POSITION AND HOLD OPERATION BY AGENT-BASED DYNAMIC RISK MODELLING

S.H. Stroeve
B.A. van Doorn
G.J. Bakker

NLR-TP-2013-489

NLR Air Transport Safety Institute
Research & Consultancy

Executive summary

SAFETY ASSESSMENT OF A FUTURE TAXI INTO POSITION AND HOLD OPERATION BY AGENT-BASED DYNAMIC RISK MODELLING

Problem area
Agent-based dynamic risk modelling supports the design of future air traffic operations by risk analysis methods that account for the performance variability of the interacting operators and systems, and the resulting emergence of safety occurrences.

Description of work
The paper shows the application of this modelling approach in a risk assessment cycle of a future A-SMGCS level 3 supported taxiing into position and hold operation.

Results and conclusions
Accident risk results have been obtained by Monte Carlo simulations of a multi-agent dynamic risk model. The uncertainty in the risk has been evaluated using sensitivity analysis and feedback of operational experts.

Applicability
Safety assessment of air traffic operations.

Report no.
NLR-TP-2013-489

Author(s)
S.H. Stroeve
B.A. van Doorn
G.J. Bakker

Report classification
UNCLASSIFIED

Date
October 2013

Knowledge area(s)
Vliegveiligheid (safety & security)

Descriptor(s)
safety
multi-agent system
dynamic risk model
air traffic management
TOPAZ

This report is based on an article published in Journal of Aerospace Operations 1 (2012) 107-127 by IOS Press.

NLR-TP-2013-489

NLR Air Transport Safety Institute

UNCLASSIFIED

NLR Air Transport Safety Institute

Anthony Fokkerweg 2, 1059 CM Amsterdam,
P.O. Box 90502, 1006 BM Amsterdam, The Netherlands
Telephone +31 88 511 35 00, Fax +31 88 511 32 10, Web site: http://www.nlr-atsi.nl

NLR Air Transport Safety Institute
Research & Consultancy

NLR-TP-2013-489

Safety assessment of a future taxi into position and hold operation by agent-based dynamic risk modelling

S.H. Stroeve
B.A. van Doorn
G.J. Bakker

This report is based on an article published in Journal of Aerospace Operations 1 (2012) 107-127 by IOS Press

Customer	National Aerospace Laboratory NLR
Owner	National Aerospace Laboratory NLR
Division	Air Transport
Distribution	Unlimited
Classification of title	Unclassified
	October 2013

Approved by:

Author S.H. Stroeve	Reviewer External anonymous review	Managing department A.D.J. Rutten
Date: 29-1-'14	Date: 29-1-14	Date: 29-1-14

Summary

Agent-based dynamic risk modelling supports the design of future air traffic operations by risk analysis methods that account for the performance variability of the interacting operators and systems, and the resulting emergence of safety occurrences. The paper shows the application of this modelling approach in a risk assessment cycle of a future A-SMGCS level 3 supported taxiing into position and hold operation. Accident risk results have been obtained by Monte Carlo simulations of a multi-agent dynamic risk model. The uncertainty in the risk has been evaluated using sensitivity analysis and feedback of operational experts.

Contents

1 Introduction

To improve future air traffic management (ATM) for accommodating expected increases in air transport, research and development programmes as SESAR and NextGen focus on development and deployment of next generation ATM in Europe and USA. For instance, the European ATM Master Plan aims to accommodate a 73% increase in flights by 2020 (w.r.t. 2005) and a further capacity increase beyond [1]. Such capacity increases should be attained while targets for other key performance indicators are respected. In particular, for safety it is demanded [1] that “the total numbers of ATM induced accidents and serious or risk bearing incidents will not increase despite traffic growth”. As a way towards increasing the ATM capacity, the RESET project [2] of the European Commission 6th Framework Programme aims to identify safe reductions in separation minima. In the RESET project several potential separation standard modifications have been suggested, including new procedures and systems for a taxi into position and hold (TIPH) operation. The phraseology standard of the International Civil Aviation Organization (ICAO) for this operation is “line up and wait”.

The safety of current as well as of future air traffic operations depends on complex and distributed interactions between human operators and technical systems, where the interactions are knowledge intensive and highly regulated by procedures. Following a long tradition in safety assessment of technical systems, air traffic operations are often assessed on the basis of fault and event trees. Fault and event trees are pictorial representations of Boolean logic relations between success and failure types of events. Event trees use forward logic, reasoning from an initiating event to its possible consequences; fault trees use backward logic, reasoning from a top event to its contributing causes. Here, risk quantification is based on (conditional) event probabilities. Recent views on accident causation indicate that fault and event trees may not be adequate to represent the complexity of modern socio-technical systems [3]-[5]. Key determinants of this complexity include the number and variety of organizational entities (human, groups, technical systems), the number and types of interdependencies between organizational entities, the degree of distribution of the entities (single/multiple locations), the types of dynamic performance of the entities (static/slow/fast), and the number and types of hazards in the organization. Limitations of fault and event trees include the difficultness to represent the large number of interdependencies between organizational entities and the dynamics of these interdependencies.

As a way forward, it was argued that for managing safety risk and resilience in complex socio-technical organizations, there is a need for analysis methods that account for the performance variability of the interacting humans and systems and the resulting emergence of safety occurrences [3]-[5]. Systemic accident modelling methods such as Functional Resonance Accident Model (FRAM) [5], Systems-Theoretic Accident Model and Processes (STAMP) [4] and Traffic Organization and Perturbation AnalyZer (TOPAZ) [6] have been developed in support of this need. The latter approach has been developed uniquely for the assessment of air traffic safety and it includes agent-based dynamic risk modelling, Monte Carlo simulation and uncertainty evaluation for assessment of risk probability levels [6]-[9].

It is the aim of this paper to highlight the TOPAZ steps in the risk assessment of the TIPH operation considered in the RESET project and to provide preliminary risk assessment results. The paper presents the model development for a particular TIPH scenario, the attained collision risk results and the parameter uncertainty in these results. Section II introduces the risk assessment cycle applied for the TIPH operation and summarizes earlier obtained results for its first steps. Section III describes the development of the dynamic risk model (DRM) of a TIPH scenario. Section IV provides a detailed account of risk point estimates arrived at by Monte Carlo simulations of the DRM. Section V gives an account of the methods and results for evaluation of the uncertainty in the risk results. Section VI provides results on the tolerability of the risk levels, the main safety bottlenecks and measures that have been identified in order to reduce the risk. Section VII discusses the results of this research.

Earlier exposure of the research in this paper was achieved at conferences [10], [11].

2 RISK ASSESSMENT CYCLE

Figure 1 shows an overview of the steps in the safety risk assessment cycle [9]. 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). 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 intended enhancements themselves.

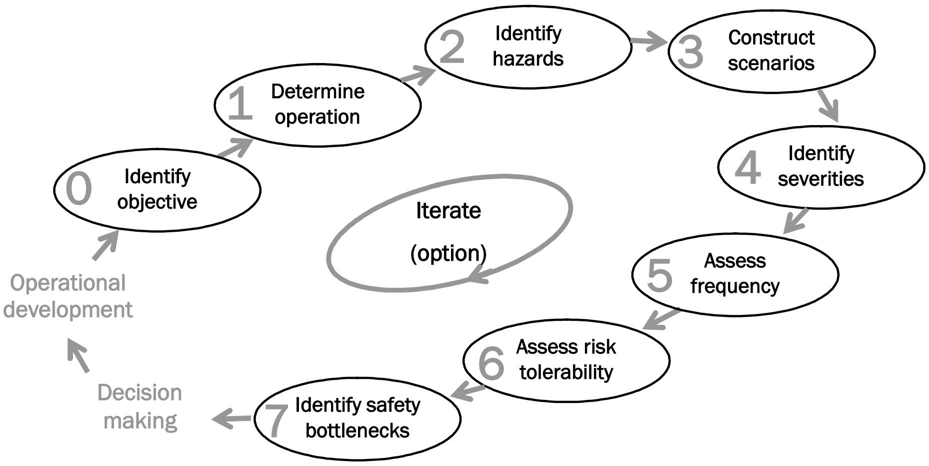

Figure 1: Steps in the safety risk assessment cycle

In the safety assessment of the RESET TIPH operation, Steps 0 to 4 served as a starting point for the development of a DRM. Key results of these steps are highlighted next, their details are presented in Ref. [12].

Step 0: Identify objective

In Step 0 safety criteria for the TIPH operation were derived. The approach followed was based on worldwide accident data for the ATC sub-products landing, line-up and take off [13]. The acquired target level of safety includes a risk reduction ambition factor of two, leading to a maximum accident risk of 3.7E-9 per flight for the TIPH operation.

Step 1: Determine operation

In Step 1 a description of the operational concept was obtained. This consolidated description serves as a starting point of the safety assessment. The TIPH operation aims at placing an aircraft on the mixed mode runway, ready for immediate departure as soon as no other restrictions apply and the departure clearance can be issued by the air traffic controller. An aircraft that has been cleared to taxi into position and hold can enter the runway after the aircraft currently using the runway (either landing or taking-off) has passed the waiting aircraft's position. Thus, the time between issuance of the departure clearance and actual start of the take-off roll can be reduced as the line-up is conducted while another aircraft is completing its landing or take-off. The TIPH procedure is applied during all visibility conditions (visibility condition 1 to 4, Ref. [14]). During visibility conditions 2, 3 and 4 A-SMGCS level 3 equipment is required. In this case, the A-SMGCS equipment includes automatic switching off the stopbar when the aircraft currently using the runway has passed the waiting aircraft, automatic detection of runway incursions using ATC surveillance data, uplink of ATC surveillance data (including runway incursion alerts) by traffic information service-broadcast (TIS-B), and presentation of this surveillance data on the cockpit display of traffic information (CDTI).

Step 2: Identify hazards

In Step 2 hazards were identified using hazard databases and hazard brainstorming sessions with pilots and controllers. Some additional hazards were identified during the scenario construction of Step 3. In total 153 hazards were identified [12], including e.g. 'wrong red stopbar is switched off', 'wrong aircraft identified', 'R/T frequency congestion', 'pilot validates without checking', 'pilot unfamiliar with airport', etc.

Step 3: Construct scenarios

In Step 3 safety relevant scenarios were constructed using the hazards identified in Step 2. These scenarios represent relations between events/conditions that may lead to potentially hazardous air traffic situations in the TIPH operation and events/conditions that may hamper resolution of these air traffic situations. Eight scenarios were identified [12], including conflict scenario 1 (CS-1) that describes the conflict between an aircraft landing and an aircraft lining up while it should not (see Figure 2). The other scenarios describe various conflict conditions between aircraft taxiing, landing, having landed and taking off.

Step 4: Identify severities

In step 4 all the safety relevant scenarios for TIPH were assessed in terms of severity. It was concluded that all eight scenarios can potentially result in an accident. It was argued [12] that CS-1 represents one of the more risky scenarios of the TIPH operation and that its risk budget should be 1.1E-9 accidents per flight, which is about 30% of the total target level of safety of the TIPH operation.

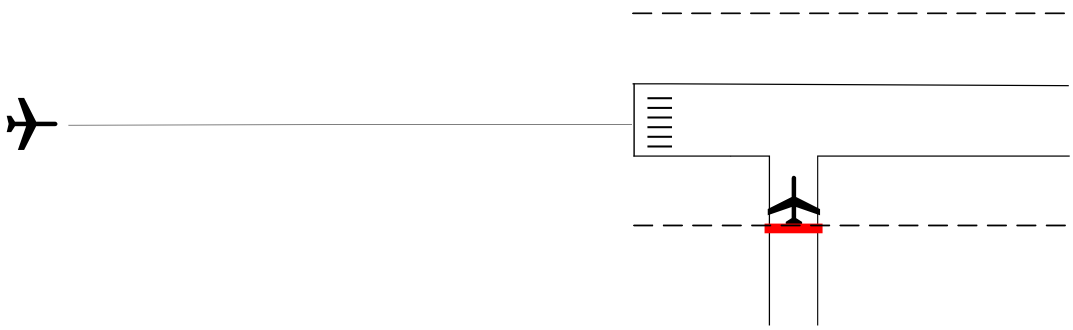

Figure 2: Schematic representation of CS-1, which considers the conflict between an aircraft landing with an aircraft lining up while it should not.

3 DYNAMIC RISK MODELLING OF TIPH SCENARIO

3.1 AGENT-BASED DYNAMIC RISK MODEL

Building forward on the results of Steps 1 to 4, the development of a dynamic risk model (DRM) was focused on the conflict scenario involving a landing aircraft and a taxiing aircraft, which is lining up on the runway while it should not (Figure 2). The development of a dynamic risk model of an air traffic scenario is based on a mathematical modelling approach, which uniquely defines the stochastic dynamics of the related agents (human operators and technical systems). This approach uses a stochastic dynamic extension of the Petri net formalism to develop an hierarchically structured representation of the agents in the air traffic scenario [15].

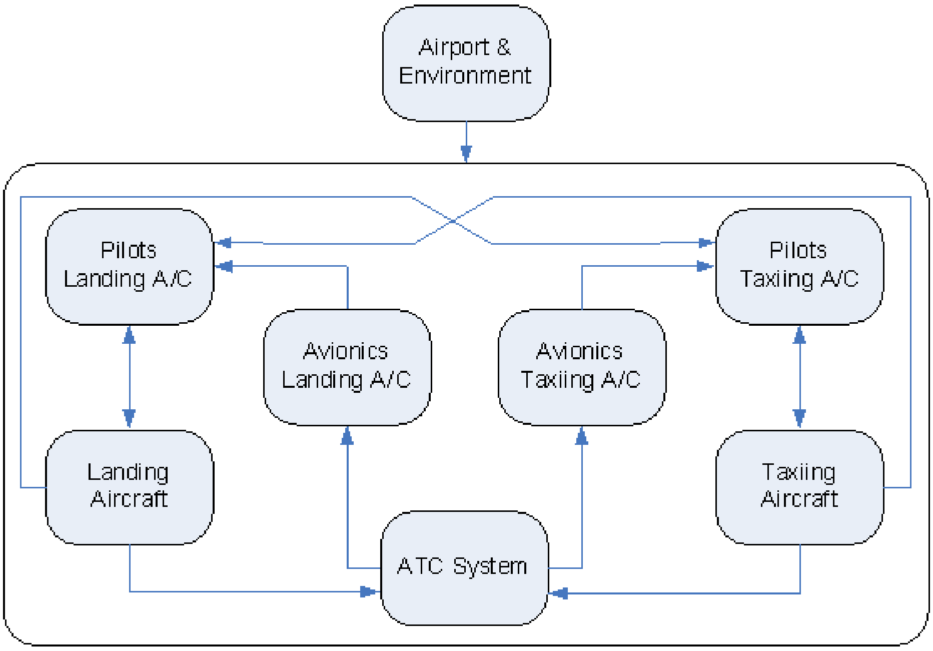

Figure 3. Agents in the DRM of the TIPH operation.

For CS-1 of the TIPH operation, the dynamic risk model includes the agents shown in Figure 3: the landing aircraft, the taxiing aircraft, the pilots of the landing aircraft, the pilots of the taxiing aircraft, the avionics of the landing aircraft, the avionics of the taxiing aircraft, the ATC system and the airport and environment. For all these agents, one or more Local Petri Nets (LPNs) are defined, which describe the agents' performance and interactions. A high-level description of these LPNs is presented next per agent; more details are reported in Ref. [16].

Landing Aircraft

The performance of the agent Landing Aircraft is modelled by two LPNs:

- Characteristics – This describes the aircraft type, its size and its landing reference speed. The aircraft type may be a medium jet or a large jet. The landing reference speed is chosen from a probability distribution that accounts for weight variances.
- Evolution – This describes the evolution of the aircraft during final approach, landing, taxiing on the runway and missed approach. The aircraft descends along the glide scope from the final approach fix to the runway threshold with lateral and vertical deviations chosen from the ICAO Collision Risk Model [17] (CRM). The aircraft flies with a constant calibrated air speed from the final approach fix up to the outer marker, it decelerates to its final approach speed between the outer marker and the deceleration point, and it progresses with a constant calibrated air speed to the runway threshold; the achieved ground speed depends on the wind. The aircraft may initiate a missed approach. The nominal missed approach path is aligned with the runway, but the achieved missed approach path includes lateral deviations in line with the ICAO CRM. The vertical missed approach path includes a speed-dependent initial height loss and a constant rate of climb thereafter. At the runway threshold, when the aircraft commences the landing, it is always at the nominal height of the instrument landing system and during the landing it has no lateral deviations with respect to the runway centreline. During the transition phase the aircraft descends with constant speed along a circle segment until touchdown. After touchdown the aircraft decelerates to taxi speed and then it progresses with constant speed on the runway. The evolution of the landing aircraft (and thereby of the conflict scenario) is ended when it has passed the position of the taxiing aircraft.

Taxiing Aircraft

The performance of the agent Taxiing Aircraft is modelled by two LPNs:

- Characteristics – This describes the aircraft type and its size. The aircraft type may be a medium jet or a large jet.
- Evolution – This describes the evolution of the aircraft during the taxi into position and hold operation as well as during manoeuvres to avoid a collision. At the start of the conflict scenario, the aircraft is located in front of

the stopbar, where it may be holding or have a line-up speed. The time at which the taxiing aircraft initiates to taxi into position is uniformly distributed in the time frame during which TIPH is not allowed (i.e. when the landing aircraft has passed a minimum distance to the runway threshold until the time that the landing aircraft has passed the taxiing aircraft). The aircraft taxies along a straight line to the runway centreline, where it decelerates and holds. To avoid a collision, the aircraft may brake or it may taxi off the runway.

Pilots Landing Aircraft

The performance of the agent Pilots Landing Aircraft is modelled by two LPNs:

- Situation Awareness – This describes the situation awareness status and updating processes. The pilots have situation awareness components about the position of the ownship and of the taxiing aircraft and about the status of the runway incursion alert. The situation awareness of the pilots is updated by visual monitoring of the environment, by monitoring of the CDTI or by an active runway incursion alert. Both visual and CDTI monitoring are done using probabilistic time intervals. The pilots can only visually observe the taxiing aircraft if it is within a range in accordance with the visibility condition and the process includes a visual observation error.
- Flight Control – This describes the control of the aircraft by the pilots. The control may be for normal final approach and landing, as described for the agent Landing Aircraft, or it may be for initiation of a missed approach. The pilots initiate a missed approach if they are aware of a runway incursion alert, or if they are aware that the taxiing aircraft is within a critical distance to the runway centreline and the own aircraft is within a critical distance to the runway threshold.

Pilots Taxiing Aircraft

The performance of the agent Pilots Taxiing Aircraft is modelled by two LPNs:

- Situation Awareness – This describes the situation awareness status and updating processes. The pilots of the taxiing aircraft have situation awareness components about the position of the ownship and of the landing aircraft, about the status of the runway incursion alert and about their intent to hold or line-up. The situation awareness of the pilots is updated by visual monitoring of the environment, by monitoring of the CDTI or by an active runway incursion alert. Both visual and CDTI monitoring are done using probabilistic time intervals. The pilots can only visually observe the landing aircraft if it is within a range in accordance with the visibility condition and the process includes a visual observation error. If the stopbar on the entry of the taxiing aircraft is off, the pilots instantaneously intend to line-up on the runway. Furthermore, the pilots may intend to line-up due to some human error (e.g. communication problem, misunderstanding, misinterpretation of the stopbar status) irrespective of the status of the stopbar.

- Flight Control – This describes the control of the aircraft by the pilots. The pilots may control a line-up process such as described for the Taxiing Aircraft agent; taxi speed, acceleration and deceleration are chosen from probability distributions. The pilots recognize a conflict with the landing aircraft if they are aware of a runway incursion alert or if they are aware that the landing aircraft is within a critical distance to the runway threshold. Given conflict awareness, the pilots stop taxiing if they are aware to be not yet within a critical distance to the runway centreline or if they are not aware of their own position, and they start to taxi off the runway if they are aware to be within a critical distance to the runway centreline.

Avionics Landing Aircraft & Avionics Taxiing Aircraft

The performance of the agents Avionics Landing Aircraft and Avionics Taxiing Aircraft are both modelled by three LPNs:

- TIS-B Local – This describes the local component of the TIS-B communication with the aircraft, including the TIS-B receiver. It may be working nominally at a constant sampling rate, interruptingly or not.
- CDTI Availability – This describes the availability of the CDTI (up / down). If it is down, the uplinked information as known by the avionics cannot be transferred to the pilots.
- Situation Awareness – This describes the uplinked traffic information as known by the avionics. This uplinked information includes the position of the other aircraft and the status of the runway incursion alert.

ATC System

The performance of the agent ATC System is modelled by six LPNs:

- Surveillance – This describes the radar surveillance of aircraft movements on the airport surface and during final approach. The radar surveillance may be working nominally, it may have false tracks or it may not be working at all. Nominally, the aircraft are regularly tracked, including normal surveillance track errors. The false track mode for the landing aircraft represents the situation that it is (falsely) positioned past the entry of the taxiing aircraft while it is actually in front of it. The false track mode for the taxiing aircraft represents the situation that it is (falsely) positioned in front of the stopbar while it is actually behind it.

- RIA Availability – This describes the availability of the runway incursion alerting system (up / down).
- RIA Mode – This describes the status of the runway incursion alert. A runway incursion alert can only become active if the runway incursion alert system is available and the surveillance system works nominally. A runway incursion alert is specified if the ATC position estimate of the taxiing aircraft is within a critical distance to the runway centreline and the ATC position estimate of the landing aircraft has passed a critical distance with respect to the runway threshold.
- Stopbar Availability – This describes the availability of the remotely controlled stopbar at the entry point of the taxiing aircraft (up / down).
- Stopbar Mode – This describes the status of the remotely controlled stopbar at the entry point of the taxiing aircraft. The stopbar is switched off in the case of a technical system failure or if the surveillance system signals that a landing aircraft has passed the runway entry, e.g. due to a false track of the landing aircraft.
- TIS-B Global – This describes the global component of the TIS-B communication (up-link) with the landing and taxiing aircraft (up / down).

Airport and Environment

The performance of the agent Airport and Environment is modelled by three LPNs:

- Visibility – This describes the visibility condition during a scenario. Three visibility conditions are considered: VC1, VC2 and a combination of VC3 and VC4. The visibility conditions are represented by maximum viewing distances in the horizontal plane.
- Runway – This describes the layout and usage of the runway and its entries. If the landing aircraft is at least a minimum distance away from the runway threshold, a taxi into position and hold operation is allowed and otherwise it is not. The TIPH scenario is considered for an entry taxiway at 500 m from the runway threshold.
- Wind – This describes the wind during the scenario. The wind at reference height is chosen stochastically; its height dependence is according to the JAR-AWO wind shear model 1.

3.2 Risk decomposition

As air traffic is a very safe means of transport, the risk of collision between two aircraft is extremely low. The assessment of such low collision risk values through straightforward Monte Carlo simulation of a DRM 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 the stochastic event sequences (including dependent events) and the conditional probabilities of such event sequences in stochastic dynamic processes. The risk decomposition for the developed DRM is based on the following components.

- The common (ATC) component of up-link of ATC surveillance data is working or is not working, denoted by $\kappa^{\text{common}}_{\text{SurvUpl},t} \in$ {Up, Down}.
- The ATC Surveillance Tracking system can be functioning nominally, it can have a false track for the landing aircraft, it can have a false track for the taxiing aircraft, or it can be down, denoted by $\kappa^{\text{common}}_{\text{Tracking},t} \in$ {Nominal, False-L, False-T, Down}.
- The ATC surveillance runway incursion alert system may be working well or not, denoted by $\kappa^{\text{common}}_{\text{RIAS},t} \in$ {Up, Down}.
- The avionics of the landing aircraft supporting up-link and presentation to the pilots of ATC surveillance data may be working or not, denoted by $\kappa^{\text{ac,L}}_{\text{Avionics},t} \in$ {Up, Down}.
- The avionics of the taxiing aircraft supporting up-link and presentation to the pilots of ATC surveillance data may be working or not, denoted by $\kappa^{\text{ac,T}}_{\text{Avionics},t} \in$ {Up, Down}.
- The intent of the pilots of the taxiing aircraft may be to hold or to line-up, denoted by $\kappa^{\text{ac,T}}_{\text{Intent},t} \in$ {Hold, Line-up}. The latter condition refers to the conflict scenario considered in this risk assessment.
- The visibility may be in either one the three conditions: 1, 2, or 3 and 4 combined, denoted by $\kappa^{\text{common}}_{\text{Visibility},t} \in$ {VC1, VC2, VC3/4}.

Combination of all risk decomposition conditions of the conflict scenario leads to 192 combinations, i.e. 64 combinations per visibility condition. Since the ATC surveillance runway incursion alert system does not provide an alert, if the ATC surveillance system is down or if it has a false track of the landing or taxiing aircraft, there remain 120 combinations of independent risk decomposition conditions (40 per visibility condition). The Monte Carlo simulations provide risk estimates for all these cases.

4 RISK POINT ESTIMATE RESULTS

Based on the developed DRM and the associated risk decomposition, various sessions of Monte Carlo simulations were performed. Per risk decomposition condition up to 1 million simulation runs were done or less if sufficient collisions had been counted. Overall results for the risk contributions of the considered visibility conditions to the total risk are shown in Table 1 below. It follows from Table 1 that the conditional collision risk given a particular visibility condition increases with about a factor three for the poorer visibility in VC2 with respect to VC1 as well as for VC3/4 with respect to VC2. Accounting for the assumed probabilities of the visibility conditions it reads in Table 1 that the largest contribution to the total risk stems from VC1 and the contributions from VC2 and VC3/4 are similar.

Table 1: Risk point estimates for the considered visibility conditions.

Visibility condition	Probability of VC	Risk point estimate given VC	Contribution to total risk	
VC1	0.95	1.46E-8	1.39E-8	81%
VC2	0.04	4.63E-8	1.85E-9	11%
VC3/4	0.01	1.32E-7	1.32E-9	8%
Total	1	1.71E-8	1.71E-8	100%

In addition to the visibility conditions, the risk decomposition is based on conditions for the ATC component of the data uplink, the ATC surveillance system, the ATC runway incursion alert system, the avionics of either aircraft and the intent of the pilots of the taxiing aircraft. Table 2 to Table 5 provide results for all relevant combinations of these conditions, aggregated over the visibility conditions. Table 2 shows the probabilities of the combinations of conditions for the conflict scenario, i.e. all the cases when the pilots of the taxiing aircraft have the intent situation awareness to line-up. Table 3 shows the conditional collision risks given these cases. Table 4 shows the contributions of these cases to the collision risk (i.e. the multiplication of the figures in Table 2 and Table 3). Table 5 shows the relative contributions of these cases to the total collision risk. The highlights of the results in these tables include the following:

- The sum of the probabilities in Table 2 is 2.71E-5, implying that according to the model overall once in every 37,000 cases that an aircraft is landing and another aircraft is ready to taxi into position and hold, the TIPH is performed while it should not, i.e. in front of the landing aircraft.

- It follows from Table 2 that there are two event combinations that are much more likely than all other. Elements R1C1 contributes for 62% of the probability of the conflict scenario and it represents the situation that the pilots of the taxiing aircraft think that they may line-up as a result of some human error (e.g. communication problem, misunderstanding, misinterpretation of stopbar status) or a stopbar failure. Element R5C1 contributes for 36% of the probability of the conflict scenario and it represents the situation that the pilots of the taxiing aircraft think that they may line-up as result of a switched off stopbar due to a false track of the landing aircraft.
- It follows from Table 4 and Table 5 that by far the largest risk contribution stems from the condition that there is a false track of the landing aircraft that is positioned past the line-up position (rows R5-R6). The sum of the contributions for this condition is 1.69E-8, which is about 99% of the total risk. As a result of this particular false track, the stopbar is switched off and it thereby initiates the conflict scenario. Moreover, this condition complicates the timely recognition of the conflict, since it implies that the runway incursion alert does not become active and the landing aircraft is not shown properly on the CDTI of the taxiing aircraft.
- It follows from element R1C1 in Table 4 and Table 5 that the risk for the case that all technical systems supporting the operation (avionics, TIS-B, radar, RIAS) are working well, contributes only for a very small extent of 5.23E-11 (0.31%) to the total risk. Table 3 shows that the conditional collision risk for this case is such that about one in every 300,000 conflicts would result in a collision (aggregated over the visibility conditions).
- It follows from Table 3 that the functioning of the ATC runway incursion alert system has a very large effect on the collision risk. Whereas the conditional risk is about 3E-6 if it is functioning well and the alert information can be properly uplinked to the aircraft (element R1C1), the conditional risk is in the order 1E-3 to 1E-2 if the runway incursion alerts system is not working properly (rows R2, R4-R10).
- It follows from comparison of the conditional risks for the situations that all technical systems are working well except for the local component of the uplink to either of the aircraft (elements R1C2 and R1C3 in Table 3), that failure of the uplink to the taxiing aircraft leads to considerably larger risk then failure of the uplink to the landing aircraft. Additional results reveal that this difference between both aircraft is especially prominent in good visibility

conditions. An explanation of this difference is the more stringent visual monitoring performance of the pilots of the landing aircraft.

- It follows from the similar conditional risks in row R2 of Table 3 that in the situation that the ATC runway incursion alert system is not working it does not matter whether the up-linking of ATC surveillance data is working or not. Since both alerts and position data are normally uplinked, it implies that the up-linking of the position data has almost no effect on the collision risk.
- It follows from comparison of the conditional collision risks in rows R5 & R6 with those in rows R7 & R8 of Table 3 that given a false track of the landing aircraft or of the taxiing aircraft, the conditional risks are similar. Thus, the larger contribution of the false track of the landing aircraft observed in Table 5 is not a result of a larger conditional risk, but due to the fact that it is a cause of the conflict scenario itself.
- It follows from comparison of the conditional collision risks in rows R5 & R7 with rows R2, R4, R6, R8, R9 & R10 of Table 3 that situations that cause the runway incursion alerting to be non-functioning due to a false track lead to lower conditional collision risks than non-functioning alerting due to failure of the surveillance system or runway incursion alert system. An explanation is that the durations of false track situations are shorter than the durations of those system failures.
- It follows from additional results that the conditional collision risks given that one or more technical systems fail during the conflict scenario, may be very high, especially in poorer visibility conditions. The conditional collision risk may be up to 3E-2 in VC1, up to 2E-1 in VC2 and up to 8E-1 in VC3/4. These results indicate that especially in VC2 and VC3/4 the avoidance of a collision when an aircraft lines up while it should not is very dependent on the well functioning of the technical systems (avionics, TIS-B, radar, RIAS); the pilots can observe the conflict visually only at a late stage (often too late).

Table 2: Probabilities of the combinations of the risk decomposition conditions leading to the conflict scenario (i.e. pilots of the taxiing aircraft intend to line-up).

Probabilities of the combinations of conditions			$\kappa^{ac,T}_{Intent}$	*Line-Up*			
			$\kappa^{ac,T}_{Avionics}$	*Up*		*Down*	
			$\kappa^{ac,L}_{Avionics}$	*Up*	*Down*	*Up*	*Down*
$\kappa^{common}_{Tracking}$	$\kappa^{common}_{SurvUpl}$	κ^{common}_{RIAS}		**C1**	**C2**	**C3**	**C4**
Nom	*Up*	*Up*	**R1**	1.67E-5	1.72E-7	1.72E-7	1.77E-9
		Down	**R2**	1.67E-9	1.72E-11	1.72E-11	1.77E-13
	Down	*Up*	**R3**	2.33E-9	2.40E-11	2.40E-11	2.48E-13
		Down	**R4**	2.33E-13	2.40E-15	2.40E-15	2.48E-17
False-L	*Up*	*Down*	**R5**	9.80E-6	1.01E-7	1.01E-7	1.04E-9
	Down	*Down*	**R6**	1.37E-9	1.41E-11	1.41E-11	1.46E-13
False-T	*Up*	*Down*	**R7**	1.67E-10	1.72E-12	1.72E-12	1.77E-14
	Down	*Down*	**R8**	2.33E-14	2.40E-16	2.40E-16	2.48E-18
Down	*Up*	*Down*	**R9**	1.67E-10	1.72E-12	1.72E-12	1.77E-14
	Down	*Down*	**R10**	2.33E-14	2.40E-16	2.40E-16	2.48E-18

Table 3: Conditional collision risks given the cases aggregated over all visibility conditions.

Conditional collision risks given the cases			$\kappa^{ac,T}_{Intent}$	*Line-Up*			
			$\kappa^{ac,T}_{Avionics}$	*Up*		*Down*	
			$\kappa^{ac,L}_{Avionics}$	*Up*	*Down*	*Up*	*Down*
$\kappa^{common}_{Tracking}$	$\kappa^{common}_{SurvUpl}$	κ^{common}_{RIAS}		**C1**	**C2**	**C3**	**C4**
Nom	*Up*	*Up*	**R1**	3.13E-06	3.96E-06	6.44E-05	1.16E-04
		Down	**R2**	2.16E-02	2.13E-02	2.21E-02	2.21E-02
	Down	*Up*	**R3**	2.45E-02	2.37E-02	2.48E-02	2.57E-02
		Down	**R4**	2.59E-02	2.54E-02	2.60E-02	2.49E-02
False-L	*Up*	*Down*	**R5**	1.68E-03	1.85E-03	1.77E-03	1.75E-03
	Down	*Down*	**R6**	2.49E-02	2.51E-02	2.65E-02	2.58E-02
False-T	*Up*	*Down*	**R7**	1.69E-03	1.65E-03	1.84E-03	1.76E-03
	Down	*Down*	**R8**	2.47E-02	2.45E-02	2.52E-02	2.53E-02
Down	*Up*	*Down*	**R9**	2.42E-02	2.38E-02	2.38E-02	2.30E-02
	Down	*Down*	**R10**	2.51E-02	2.50E-02	2.49E-02	2.49E-02

Table 4: Risk contributions of the cases aggregated over all visibility conditions.

Risk contributions of the cases			$\kappa^{ac,T}_{Intent}$	*Line-Up*			
			$\kappa^{ac,T}_{Avionics}$	*Up*		*Down*	
			$\kappa^{ac,L}_{Avionics}$	*Up*	*Down*	*Up*	*Down*
$\kappa^{common}_{Tracking}$	$\kappa^{common}_{SurvUpl}$	κ^{common}_{RIAS}		**C1**	**C2**	**C3**	**C4**
Nom	*Up*	*Up*	**R1**	5.23E-11	6.80E-13	1.11E-11	2.06E-13
		Down	**R2**	3.61E-11	3.67E-13	3.80E-13	3.91E-15
	Down	*Up*	**R3**	5.72E-11	5.70E-13	5.96E-13	6.38E-15
		Down	**R4**	6.04E-15	6.10E-17	6.25E-17	6.17E-19
False-L	*Up*	*Down*	**R5**	1.65E-08	1.87E-10	1.78E-10	1.81E-12
	Down	*Down*	**R6**	3.41E-11	3.53E-13	3.74E-13	3.77E-15
False-T	*Up*	*Down*	**R7**	2.82E-13	2.83E-15	3.17E-15	3.11E-17
	Down	*Down*	**R8**	5.77E-16	5.89E-18	6.04E-18	6.27E-20
Down	*Up*	*Down*	**R9**	4.04E-12	4.09E-14	4.09E-14	4.07E-16
	Down	*Down*	**R10**	5.86E-16	6.00E-18	5.98E-18	6.18E-20

Table 5: Relative risk contributions of the cases aggregated over all visibility conditions.

Relative risk contributions of the cases			$\kappa^{ac,T}_{Intent}$	*Line-Up*			
			$\kappa^{ac,T}_{Avionics}$	*Up*		*Down*	
			$\kappa^{ac,L}_{Avionics}$	*Up*	*Down*	*Up*	*Down*
$\kappa^{common}_{Tracking}$	$\kappa^{common}_{SurvUpl}$	κ^{common}_{RIAS}		**C1**	**C2**	**C3**	**C4**
Nom	*Up*	*Up*	**R1**	0.31%	0.00%	0.06%	0.00%
		Down	**R2**	0.21%	0.00%	0.00%	0.00%
	Down	*Up*	**R3**	0.33%	0.00%	0.00%	0.00%
		Down	**R4**	0.00%	0.00%	0.00%	0.00%
False-L	*Up*	*Down*	**R5**	96.68%	1.10%	1.04%	0.01%
	Down	*Down*	**R6**	0.20%	0.00%	0.00%	0.00%
False-T	*Up*	*Down*	**R7**	0.00%	0.00%	0.00%	0.00%
	Down	*Down*	**R8**	0.00%	0.00%	0.00%	0.00%
Down	*Up*	*Down*	**R9**	0.02%	0.00%	0.00%	0.00%
	Down	*Down*	**R10**	0.00%	0.00%	0.00%	0.00%

Above results provide insight in the contributions of the conditions used in the risk decomposition. Additional insights can be obtained by assessing the risk for variations in values of parameters of the DRM. Figure 4 shows the collision risk graphs for the various visibility conditions in consideration of variations in six parameter values. These parameters reflect the performance of technical systems and human operators, as well as the geometry of the runway strip.

- Figure 4a shows the collision risks as function of the probability of a false track of the landing aircraft. It follows that the collision risks are about linearly related to the false track probability, since in this parameter range the collision risks are almost completely determined by this false track condition.
- Figure 4b shows the collision risks as function of the mean duration of the false track of a landing aircraft. It follows that with respect to the nominal value of 10 seconds, a decrease has a stronger effect on the risk than an increase.
- Figure 4c shows the collision risks as function of the mean time between visual monitoring by the pilots of the taxiing aircraft. The three parameter values may be considered as the following cases: 1 second indicates monitoring frequently; 17 seconds indicates monitoring once after start of line-up; 300 seconds indicates no monitoring after start of line-up. It follows from Figure 4c that the total risk decreases by about a factor 10 if monitoring would be done frequently rather than once after start of the line-up. The risk estimates depend strongly on the visibility condition. In VC1 the risk becomes very low, whereas in VC2 and VC3/4 the risk is not very sensitive for the monitoring performance.
- Figure 4d shows the collision risks as function of the distance of the taxiing aircraft to the runway centre-line where it is recognized as conflicting by the pilots of the landing aircraft. It follows that the collision risk estimates are only a bit higher if the decision distance would be 25 m rather than the nominal value of 62 m. However, if the conflict would already be recognized if the taxiing aircraft would just have passed the stopbar (at 153 m) than the total risk would decrease largely. For this large distance, reduced visibility (VC2 and VC3/4) has a large effect on the total risk.
- Figure 4e shows the collision risks as function of the distance of the stopbar to the runway centre-line. It follows that the risk increases strongly if the stopbar and runway-holding position are closer to the runway. According to ICAO Annex 14 the minimum distance of the runway holding point with respect to the runway centre-line is 90 m for CAT I, II or III precision approaches [19]. For CAT II en III precision approaches the required distance may be larger, but no standard distances are specified in ICAO Annex 14,

rather they have to be determined based on the size of the ILS critical and sensitive areas. A typical distance is CAT II/III runway holding position is just outside the runway strip, which has a width of 150 m at both sides of the runway centre-line. It follows from Figure 4e that if the stopbar is at the minimum distance of 90 m rather than at the typical distance just outside the runway strip, then the risk estimate is about a factor 10 higher for all visibility conditions.

- Figure 4f shows the collision risks as function of the distance of the runway entry with respect to the runway threshold. It follows that the risk would be less if the runway entry would be directly at the runway threshold rather than at a more remote position. An explanation is that in the model part of the landing aircraft have sufficient height to fly over the taxiing aircraft at the threshold position.

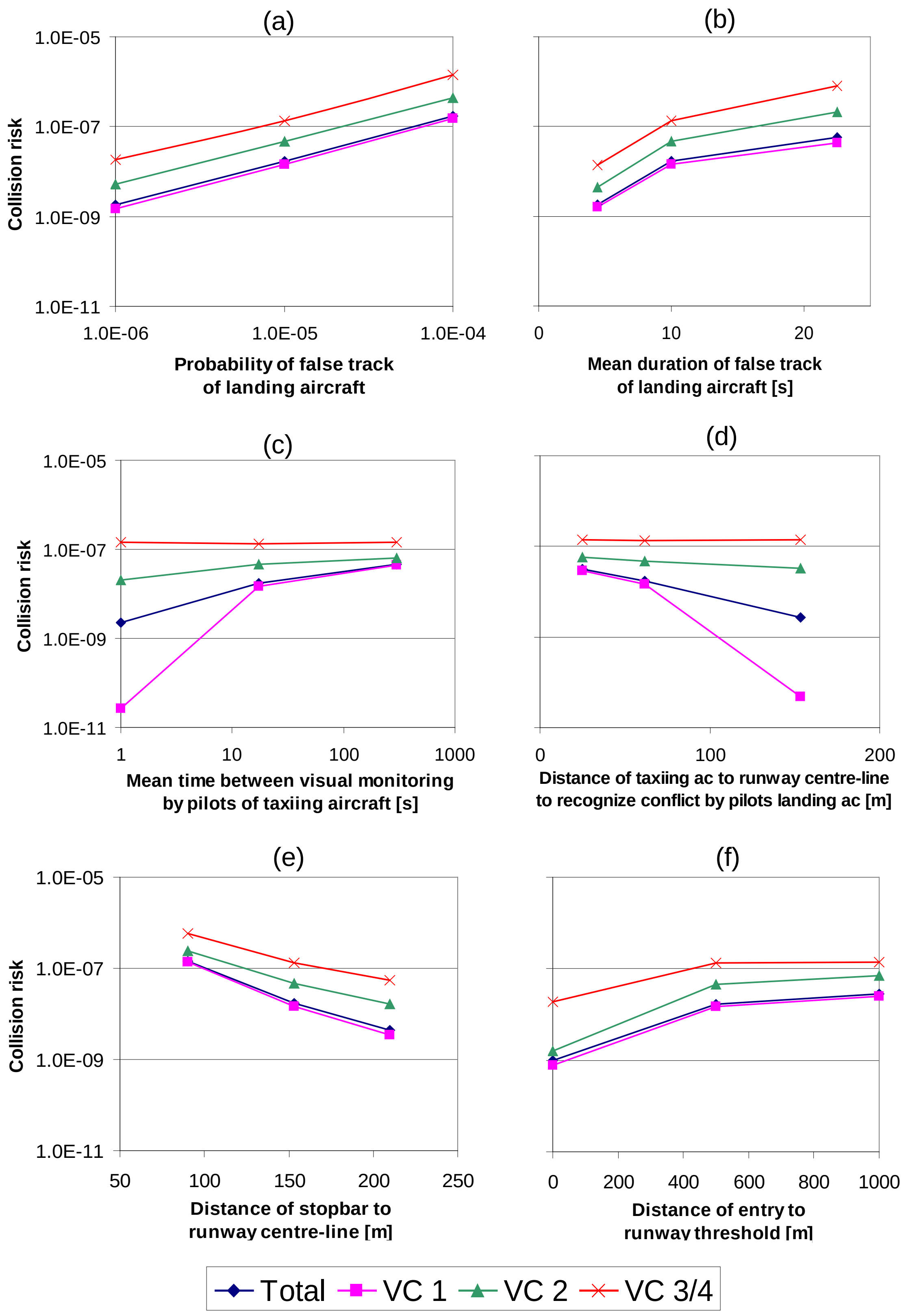

Figure 4: Collision risk graphs for variations of parameters as explained in the main text. Each graph shows the total risk and the conditional risks given the visibility conditions.

5 BIAS AND UNCERTAINTY ASSESSMENT

5.1 METHODS

By definition, any model differs from reality. As an integrated part of TOPAZ, a bias and uncertainty assessment method has been developed [8],[18]. This method supports identification of differences between the DRM and reality, and subsequent evaluation of the bias and uncertainty in the risk outcomes due to these differences. It consists of the following steps:

1. *Identify all potential differences between the simulation model and reality.* During the development of a dynamic risk model assumptions are adopted and explicitly written down. The parameter assumptions regard the values adopted for all parameters of the DRM, e.g. values of event probabilities, moments of probability distributions, geometry data, etc. The non-parameter assumptions regard all other assumptions, e.g. the types of situation awareness of an agent, the decision strategies of agents, the types of probability distributions, the representation of the dynamic performance of agents, the representation of all hazards in the model, etc. All assumptions are potential differences between the DRM and reality.
2. *Assess the size/probability of each difference.* For each difference it is assessed how large it is or how often it may happen. For each parameter value a 95% uncertainty interval is assessed by the median and the size of the interval; this median may be biased with respect to the parameter value. In support of this assessment, the following ordered categories of the sizes of bias factors and uncertainty intervals are used: Neutral, Negligible, Small, Minor, Significant, Considerable, Major. These categories reflect differences of less than about 10% to more than about a factor 10. For each non-parameter assumption, the probability is assessed that the assumption reflects a difference with respect to reality.
3. *Assess the risk sensitivity for changes in parameter values.* The normalized sensitivities of the risk outcomes of the DRM for changes in the parameter values are assessed. This assessment may be done by a DRM expert using knowledge of the model and qualitative sensitivity categories (Negligible, Small, Minor, etc.). For critical parameters it is done by additional Monte Carlo simulations in which the effects of parameter variations are explicitly evaluated.
4. *Assess the effect of each difference on the risk outcome.* The uncertainty interval of each parameter value is combined with the risk sensitivity to find

the uncertainty interval in the risk for the parameter value considered. The effect on the risk uncertainty interval can only be large if the parameter uncertainty interval and the risk sensitivity are sufficiently large. For each non-parameter assumption, a conditional risk bias given that it represents a difference, is assessed. The probability that the difference exists and the conditional risk bias are combined to a risk bias for each difference.

5. *Determine the joint effects of all differences.* The assessment results for all individual differences are combined via bias and uncertainty assessment methods [8],[18] to best estimates of the risk and its uncertainty interval.

Details of above steps in the preliminary risk assessment of the TIPH scenario are as follows.

- For project-related reasons, it was decided to restrict the bias and uncertainty assessment to the parameter value assumptions. This implies that a systematic assessment of the non-parameter assumptions is out of the scope of this study and that the risk results are to be considered preliminary.
- A first assessment phase was performed by the safety modelling experts. Here the uncertainty interval and risk sensitivity of all 168 parameters were assessed, leading to an assessment of their effect on the risk for each parameter. This assessment was done conservatively, in order to not falsely judge the risk uncertainty as being too low. The result of this phase is a list of 118 parameters with a Neutral or Negligible risk effect and a list of 50 parameters with a (potentially) more than Negligible effect on the risk.
- For all parameters that had been assessed in the first phase to have a more than Negligible risk effect, a second assessment of the parameter uncertainty interval was performed. For most parameters, this was done based on structured feedback of operational experts, for some parameters searches in the literature and safety databases were performed. The feedback of operational experts was obtained via questionnaires and interviews. The questions asked relate to the performance of pilots, controllers and systems in normal circumstances as well as in the specific context of the conflict scenario. In this study we obtained feedback from two airline pilots, two active air traffic controllers and one former air traffic controller.
- For all parameters that had been assessed in the first phase to have a more than Negligible risk effect, dedicated Monte Carlo simulations were performed to assess the risk sensitivity more precisely.

5.2 RESULTS

In the bias and uncertainty assessment, we assessed the uncertainty interval of each parameter value, the risk sensitivity of each parameter value and the combined effect on the risk uncertainty level. The 95% uncertainty interval of the total risk that follows from this assessment is [2.16E-10, 1.35E-6], i.e. the total risk resides with 95% probability in an interval from a factor 79 below to a factor 79 above the point estimate of the risk.

Table 6 shows the parameters with the most important contributions to the risk uncertainty and risk sensitivity. It can be seen in this table that there are four parameters with a risk uncertainty contribution being Major or Considerable. The uncertainty in these parameters contributes to the risk uncertainty interval being a factor 36 above and below the risk point estimate; all other parameters contribute only an additional factor 2.2.

- Both the probability and the mean duration of a false track of the landing aircraft have a large risk sensitivity (see Figure 4a,b) and a large effect on the risk uncertainty. The large risk sensitivity is due to a combination of contributions: (1) the considered type of false track (past the waiting aircraft) leads to dimming of the stopbar, (2) it implies that no runway incursion alert is specified to either of the aircraft and (3) it implies that the landing aircraft is falsely positioned on the CDTI of the taxiing aircraft. We obtained feedback from a controller that false tracks are quite common and occur almost daily in some form; he did however not know cases of the particular false track situation considered. We did not have access to radar track data or failure reports. The large uncertainty about these false tracks is reflected in the assessment.
- The visual monitoring performance of the pilots of the taxiing aircraft has a large effect on the uncertainty in the risk level. The two pilots that we interviewed had quite contrasting opinions: one of the pilots argued that during lining-up the pilots very regularly monitor the traffic situation, whereas the other pilot argued that given that the pilots think that lining-up is allowed and safe (i.e. an aircraft is approaching at sufficient distance) then the pilots would no longer look to the movement of the approaching aircraft. We consider both approaches to be plausible and therefore regard the monitoring performance to be very uncertain. As follows from Figure 4c, the risk sensitivity for the monitoring performance is quite large, especially in visibility condition 1, where the pilots have the possibility to well perceive a conflict at an early stage.

- The pilots of the landing aircraft need to decide when they regard the taxiing aircraft as so conflicting that they will initiate a missed approach. Both interviewed pilots indicated that the taxiing aircraft would certainly be recognized as conflicting if its nose would be at the runway edge. They differed in opinion about the maximum distance where the conflict situation would be recognized: one of the pilots argued that the aircraft would certainly not be recognized as conflicting if it would be at more than 50 m from the runway edge, while the other pilot argued that it might already be recognized as conflicting if it would have passed the position of the remotely controlled stopbar (at 153 m from the runway centre-line). As follows from Figure 4d the risk is very sensitive for this decision distance, especially in visibility condition 1.

Table 6: Parameters with a risk sensitivity or risk uncertainty of Significant or more.

Parameter	**Explanation**	**Parameter uncertainty**	**Risk sensitivity**	**Risk uncertainty**
$p_{\mathrm{Surv,ATC}}^{\mathrm{FTL}}$	Probability of false track of landing aircraft in ATC surveillance system	Major	Significant	Major
$\mu_{\mathrm{Surv,ATC}}^{\mathrm{FTL,nom}}$	Mean duration of false track of landing aircraft in ATC surveillance system	Significant	Major	Major
$\mu_{\mathrm{Pl,T}}^{\mathrm{Mon,vis}}$	Mean time until next SA update via visual monitoring by the pilots of the taxiing aircraft	Major	Significant	Major
$d_{\mathrm{Pl,L}}^{\mathrm{conflict,T}}$	Distance of the taxiing aircraft to the runway centre-line within which it is recognized as conflicting by the pilots of the landing aircraft	Significant	Considerable	Considerable
$y_{\mathrm{TIPH}}^{\mathrm{min,ac\text{-}L}}$	Minimum distance of landing aircraft to runway threshold such that TIPH may be initiated	Minor	Significant	Minor

Parameter	Explanation	Parameter uncertainty	Risk sensitivity	Risk uncertainty
$d_{\mathrm{Pl,T}}^{\mathrm{stop,ac\text{-}T}}$	Minimum distance of the taxiing aircraft in front of the runway where the pilots of the taxiing aircraft initiate stopping	Minor	Significant	Minor
$\mu_{\mathrm{Pl,T}}^{v,\mathrm{line\text{-}up}}$	Mean taxi speed during line-up	Small	Considerable	Minor
$d_{\mathrm{RIA,ATC}}^{\mathrm{ac,T}}$	Threshold distance of taxiing aircraft w.r.t. runway centre-line for runway incursion alert activation	Small	Significant	Small
$p_{\mathrm{AC,T}}^{\mathrm{hold}}$	Probability that taxiing aircraft initiates the runway line-up from hold	Negligible	Significant	Negligible

6 RISK TOLERABILITY, SAFETY BOTTLENECKS AND MITIGATING MEASURES

In Step 6 of the safety risk assessment cycle the risk tolerability is assessed by comparing the risk results with the risk criteria. Table 7 shows this comparison for the preliminary risk results obtained and the adopted target level of safety (TLS). It is manifest that the risk point estimates and a large part of the risk uncertainty interval are well above the TLS; only the lower bound of the risk uncertainty interval of the total risk is a bit below the TLS. Given the preliminary nature of the risk assessment results, we assess the risk to be potentially unacceptable.

Table 7: Comparison of preliminary risk assessment results with the target level of safety for Scenario 1 of the TIPH.

Risk metric	Risk value	Factor w.r.t. TLS
Target level of safety	1.1E-9	1
Risk point estimate for VC1	1.46E-8	13.3
Risk point estimate for VC2	4.64E-8	42.2
Risk point estimate for VC3/4	1.32E-7	120
Point estimate of total risk	1.71E-8	15.5
95% Uncertainty interval of total risk	[2.16E-10, 1.35E-6]	[0.196, 1230]

In Step 7 of the safety risk assessment cycle the main sources contributing to unacceptable safety levels are identified; these sources are entitled ‘safety bottlenecks’. Since we assessed the risk as potentially unacceptable, we identified potential safety bottlenecks. The derivation of the potential safety bottlenecks is based on the largest risk contributions of Table 4 and the parameters with the risk sensitivity or risk uncertainty being at least Considerable in Table 6. The potential safety bottlenecks based on these highest ranking risk results are the following ones.

- False surveillance data of the landing aircraft may cause false automatic switching of the stopbar and non-functioning of the runway incursion alert system.
- Pilots may not continue monitoring for potential conflicts after they started taxiing into position.

- Pilots may decide to initiate a missed approach only if they observe that a taxiing aircraft is very close to the runway.
- The taxi speed during line-up may be too high.

The results of the safety risk assessment cycle, including the accident risk levels, the risk sensitivities, the risk tolerability's and the safety bottlenecks, support further development of the TIPH operational concept. As an onset, a brainstorm was organized to identify mitigating measures that have the potential to reduce the risk levels assessed. The workshop started with a presentation of the main safety findings identified and the brainstorm was structured by the four safety bottlenecks presented above. The brainstorm participants included pilots, controllers, A-SMGCS experts, HF experts and safety experts, and they were asked to come up with ideas on potential mitigating measures in a joint session. After the brainstorm session, the arguments provided were structured in potential risk mitigations. For each of these potential risk mitigations, an initial assessment was done, including a discussion of its potential advantages and disadvantages [16]. In summary, the following potential risk mitigating measures were identified:

1. The flight crew of the landing aircraft will broadcast by radio "[ID] TOUCHDOWN RWY[xx]", once the aircraft has completed the flare and touchdown and the crew has reasonable certainty that it has passed any other aircraft on holding points for that runway.
2. Install one or more devices at the airport of which the position is known and that constantly transmit as if they were actual targets. The system will be required to continuously check the position of these devices in order to detect failures in both the surveillance subsystems and the data processing system, and alert the actors.
3. Manual switch-off of the stopbar lights by ATC.
4. Change the existing procedure for the taking-off aircraft that starts the TIPH procedure, to delay the execution of the departure/take-off checklist until lining-up has been completed. Do not execute the checklist while you are lining-up, continue to monitor for other traffic instead. Start with the checklist only when it is absolutely useless to continue to verify that you are free of conflicts.
5. Require the A-SMGCS level 3 system to:
    - Be able to identify when the holding aircraft has initiated the line-up or has surpassed the safe distance to the runway in case the aircraft has surpassed the holding point;
    - Automatically transmit clear unambiguous information to the actors (ATC and flight crews).

6. Introduce additional sensors around runway entry points (pressure, volumetric, noise, etc.).
7. Add additional display/representation of information on cockpit for landing aircraft.
8. Obligate the taking-off aircraft to make a full-stop before being able to initiate the TIPH procedure.
9. The taking-off aircraft will broadcast “[ID/AC] Entering RWY XX” to signal any other aircraft, especially landing aircraft, when they are going to start the TIPH procedure.
10. Use independent data for automatic switching of the stopbar lights and the surveillance of the traffic. For instance, radar and LMAT data may be used for the automatic switching of the stopbar lights, whereas aircraft navigation data may be shared between involved aircraft by ADS-B and this shared data may be the basis for the on-board generation of a runway incursion alert; this alert may also be down-linked to ATC.

7 Discussion

In this paper we presented a risk assessment of a novel air traffic operation based on dynamic risk modelling. In contrast with conventional fault and event trees-based risk assessment, the applied dynamic risk model explicitly represents the stochastic dynamic performance of a variety of interacting agents in an air traffic scenario, the variability of the agents' performance and the emergence of accidents in Monte Carlo simulations of the dynamic risk model. The stochastic dynamic performance of the agents considers a wide scope of aspects, including aircraft flight and taxiing performance, situation awareness updating and decision making by pilots, and the performance of A-SMGCS systems in nominal and non-nominal conditions. As would also be the case in fault/event tree analysis, the dynamic risk model includes a variety of event probabilities, for instance for the probability of events such as non-functioning of technical systems and pilot errors. In addition to such event probabilities and in contrast to the parameters used in fault/event tree analysis, the dynamic risk model includes a large number of other parameters related to performance aspects such as aircraft dynamics, timing of situation awareness updating, timing of communication, accuracy and timing of surveillance systems, decision making by pilots and A-SMGCS alert settings. Typically, such parameters can be interpreted and reflected on by operational and design experts more easily than event probabilities. This was also confirmed in the feedback obtained from pilots and controllers that contributed to this safety case.

The risk results presented in this paper are to be regarded as preliminary, since the design of the TIPH operation is at an early stage and no assessment of the non-parameter assumptions has been performed. For instance, a limitation of the developed DRM is that the runway controller has not yet been included. In the context of the risk assessment, it implies that the assumption 'The runway controller has no effect on the prevention of an accident in the conflict scenario' would have to be assessed. Here it would have to be assessed how and when the controller might recognize and react to the conflict, and in what number of cases the controller might warn the pilots of one or both aircraft before the pilots have already recognized the conflict themselves independently. Although this assumption can be classified as being safety conservative, the risk reduction as result of controller performance might well be quite limited. Reasons are that the contribution of the controller was found to be very small in good visibility in other runway incursion scenarios [20] and that both the pilots and the controller use the same surveillance and alert data in all visibility conditions, thus limiting the potential added contribution of the controller.

The results obtained show that the risk point estimates and a large part of the risk uncertainty interval are above the adopted target level of safety for the conflict scenario considered in the particular design of the A-SMGCS level 3 supported taxi into position and hold operation. In addition to the risk tolerability results, the assessment provided detailed feedback on the contributions of conditions, systems and humans to the accident risk of the conflict scenario considered. Key safety insights for the TIPH operation are:

- By far the largest risk contribution stems from the situation concerning a false track of the landing aircraft that is positioned past the line-up position: as a result the stopbar is switched off, the runway incursion alert does not become active and the landing aircraft is not shown properly on the CDTI of the taxiing aircraft.
- The functioning of the runway incursion alert system in combination with the up-linking of the alert data has a very large effect on the accident risk. When functioning properly these systems largely reduce the accident risk. Their risk reducing effect is larger than was assessed previously for a conflict between aircraft taxiing and taking off [20].
- The conditional accident risks increase considerably in poorer visibility conditions and the dependability on the proper functioning of the technical systems is very high in poor visibility.

In this study a total of ten potential measures were identified that aim to mitigate the safety bottlenecks and to reduce the accident risk in the conflict scenario. These ten potential mitigating measures provide a good opportunity to improve the TIPH design. The effectiveness of these mitigating measures may be assessed in one or more additional risk assessment cycles until it is decided that the risk of the operation is acceptable. In this way, safety targets for future operations envisioned in design programmes as SESAR and NextGen can be controlled systematically, such that also next generations of passengers can keep having safe flights back home.

8 REFERENCES

[1] SESAR. European Air Traffic Management Master Plan. Edition 1, 30 March 2009

[2] http://reset.aena.es

[3] Hollnagel E, Woods DD, Leveson N (eds.). *Resilience engineering: Concepts and precepts.* Ashgate, Aldershot, England, 2006

[4] Leveson N. A new accident model for engineering safer systems. *Safety Science* 42:237-270, 2004

[5] Hollnagel E (2004). *Barriers and accident prevention.* Ashgate, Hampshire, UK

[6] Blom HAP, Bakker GJ, Blanker PJG, Daams J, Everdij MHC, Klompstra MB. Accident risk assessment for advanced air traffic management. In: Donohue GL and Zellweger AG (eds.), *Air Transportation Systems Engineering*, AIAA, pp. 463-480, 2001

[7] Stroeve SH, Blom HAP, Bakker GJ. Systemic accident risk assessment in air traffic by Monte Carlo simulation. *Safety Science* 47:238-249, 2009

[8] Everdij MHC, Blom HAP, Stroeve SH. 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, 2006

[9] Blom HAP, Stroeve SH, De Jong HH. 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, 2006

[10] Stroeve SH, Van Doorn BA, Bakker GJ. Safety assessment of a future taxi into position and hold operation by agent-based dynamic risk modelling. 1st International Air Transport and Operations Symposium, Delft, The Netherlands, 14-15 April 2010

[11] Stroeve SH, Van Doorn BA, Bakker GJ. Studying the safety of a future taxi into position and hold operation by agent-based dynamic risk modelling. Eurocontrol Safety R&D Seminar, Brétigny-sur-Orge, France, 19-20 October 2010

[12] Brazdilova SL. Qualitative hazard analysis report, Part 1: Taxi Into Position and Hold. RESET D7.3, version 2.0, 20 April 2010

[13] Van den Bos JC, Jansen RBHJ, De Jong HH. Apportioned ATC safety criteria based on accident rates. Air Traffic Control Quarterly 17(3):269-299, 2009

[14] ICAO, Advanced Surface Movement Guidance and Control System (A-SMGCS) Manual. Doc 9830, AN/452, edition 1, 2004

[15] Everdij MHC, Klompstra MB, Blom HAP, Klein Obbink B. ‘Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets’, H.A.P. Blom, J. Lygeros (eds.), *Stochastic hybrid systems: Theory and safety critical applications*, Springer, 2006, pp. 325-350

[16] Stroeve SH, van Doorn BA, Bakker GJ, Nieto JI. Preliminary Safety Case Part I: Taxi Into Position and Hold. RESET D7.4, version 1.1, 2 November 2010

[17] ICAO. Manual on the use of the Collision Risk Model (CRM) for ILS operations. ICAO Doc 9274-AN/904, first edition, 1980

[18] Everdij MHC, Blom HAP. Bias and uncertainty modelling in accident risk assessment. European Commission project Hybridge, deliverable D8.4, 24 February 2005

[19] ICAO. Annex 14 to the Convention on International Civil Aviation: Aerodromes, Volume I, Aerodrome Design and Operations. Fifth Edition, July 2009

[20] Stroeve SH, Bakker GJ, Blom HAP (2007). Safety risk analysis of runway incursion alert systems in the tower and cockpit by multi-agent systemic accident modelling. *Proceedings 7th USA/Europe Air Traffic Management Seminar*, Barcelona, Spain, 2-5 July 2007