Using Dynamic Risk Modelling in Single European Sky Air Traffic Management Research (SESAR)

N. Fota
SESAR & Research – Performance & Method Unit EUROCONTROL, France

M.H.C. Everdij & S.H. Stroeve
National Aerospace Laboratory (NLR), Netherlands (on behalf of DFS Deutsche Flugsicherung, Germany)

T. Kråkenes & I. Herrera
SINTEF, Norway

J. Quiñones
Safety Directorate, AENA, Spain

T. Contarino & A. Manzo
SELEX & SICTA (on behalf of ENAV), Italy

ABSTRACT: The SESAR research & development programme aims to drastically change Air Traffic Management (ATM) in the European airspace. The SESAR project "Develop techniques for Dynamic Risk Modelling (DRM)" aims at demonstrating the need for and potential added value of DRM in the safety assessment of new developments. The main deliverable is a DRM guideline that will help safety practitioners to decide whether DRM modelling is expected to provide added value, and how to conduct the assessment. The added value of DRM is being demonstrated by its application to a SESAR test case.

1 INTRODUCTION

1.1 *The need for dynamic risk modelling*

Today's challenge is that aviation systems are large-scale, complex and dynamic. New automated tools are developed to assist air traffic controllers and pilots to reduce separation. These technologies introduce a change in the human-machine interface and increase the complexity of air traffic management (ATM) (Averty et al. 2009). New technology and new ways of interacting may have significant safety effects, which must be assessed by means of suitable methods.

Traditional methods such as fault trees and event trees have important limitations when it comes to capturing the dynamics and complexity of many sociotechnical systems and operations. Such "static" methods are often still adequate for some applications, but may be insufficient when faced with applications in which (Eurocontrol 2009):

a) There are multiple conditions affecting system response and operator behaviour.
b) There are different ways in which human operators may perform a task incorrectly, and there are multiple dynamic responses of the system and human operators to these different errors.
c) The physical status evolution has an influence on the stochastic discrete events related to failure and recovery.
d) There are multiple time-dependent interactions between the system and its environment, and between the system elements themselves.
e) There are uncertainties due to inherent randomness or unpredictable variability or due to the imperfect knowledge or incomplete information.

In the last decade, theories and methods have started to explicitly acknowledge dynamic sequencing and the need to address time-dependent interactions. In this paper, these methods are referred to as *Dynamic Risk Modelling (DRM)*. DRM is defined as the class of risk modelling techniques that explicitly represent the dynamic performance of the elements in the operation (people, equipment, procedures, environment) and their time-dependent interactions.

1.2 *SESAR and the DRM project*

SESAR (Single European Sky ATM Research) aims to eliminate the fragmented approach to European ATM, transform the ATM system and synchronize all stakeholders. ATM systems delivered in the scope of SESAR are increasingly complex and integrated. There is a need for more advanced safety assessment approaches, taking into account the dynamic nature of events preceding an incident/accident within a SESAR Safety Assessment, and for complementary models that account for technical and human, context, interactions and dynamics. This is the focus of SESAR DRM project (DRM project, Herrera et al.), which considers existing and emerging developments in the area of dynamic risk modelling. The main objective of the DRM project is to provide guidelines for ***when*** and ***how*** to apply DRM techniques in real world analysis

situations. These guidelines are aimed to be included in a future edition of the SESAR Safety Reference Material (SRM) (SESAR SRM 2012).

1.3 *Organisation of the paper*

This paper is organized as follows: Section 2 explains the criteria that have been developed by the DRM project for deciding whether a given SESAR application requires the use of DRM, and it explains how the DRM project has applied these criteria to select a SESAR test case application. Section 3 explains the process that led to the selection of one particular DRM method from a list of candidate methods. Section 4 briefly explains this DRM method in steps, and presents preliminary results of its application to the test case selected in Section 2. Section 5 presents concluding remarks.

2 CRITERIA FOR APPLYING DRM

The SESAR safety assessment approach typically uses static risk modelling techniques: safety criteria and objectives are identified based on accident incident models and further safety requirements are derived using Fault Trees, Failures Modes and Effects Analysis or similar techniques. This section presents criteria to identify specific cases where DRM application is required.

Criterion 1: In SESAR an initial risk evaluation using a conventional (static) method has been conducted and the level of uncertainty in the risk results is such that it cannot be conclusively argued whether the risk is acceptable or not.

Criterion 2: The system behaviour, when considering equipment functional variability, failures, human performance variability and errors, involves occurrences which cannot be considered in isolation, as they strongly depend on system status over time.

Criterion 3: The system behaviour when considering equipment functional variability, failures, human performance variability and errors depends on process variables.

If Criterion 1 is fulfilled together with at least one of Criteria 2 or 3, it is considered that the case is eligible to risk assessment with a DRM method. The anchoring points in a preceding conventional static analysis need to be clearly identified (i.e. the Operational Hazards that will be specifically modeled with DRM, their severities and associated safety objectives together with the justifications developed during the static safety risk assessment). This will serve as the basis for developing the Dynamic Risk Modelling cycle.

The DRM project applied these criteria to SESAR concepts and as a result it selected the use case "Land vs Line up" within the Conflicting ATC clearances project P06.07.01. Conflicting ATC Clearance (CATC) detection is a system that detects early situations of conflicting clearances that, if not corrected would end up in hazardous situations. The "land vs line up" use case considers one aircraft landing and another aircraft lining up to take off on the same runway used in mixed mode. For the detection to work, the controller needs to inform the system (input) each time he provides a clearance to an aircraft. In case of a "land vs line-up" CATC alert, the controller shall resolve the hazardous situation (i.e. avoid a runway collision) by immediately cancelling the line-up instruction and/or instructing a go around, as appropriate.

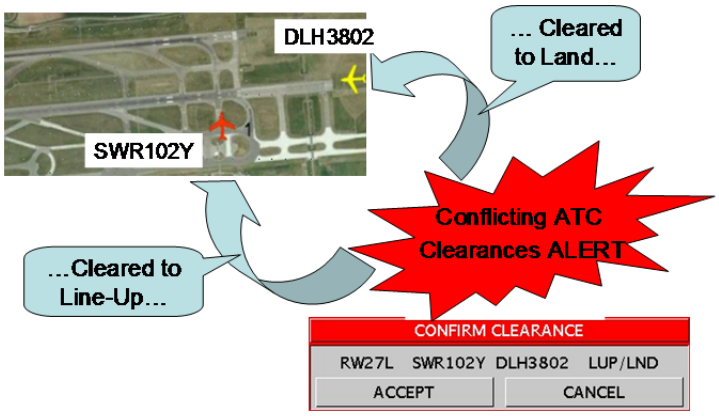

Figure 1. The land vs line-up CATC alert operation.

The static safety assessment initially performed within the SESAR project (SAR CATC 2012) identified a major uncertainty w.r.t. the efficiency of the operational use of "land vs line-up" CATC alert, in relation to the time required for the controller to interpret the alert and communicate the resolution instruction(s) to the involved aircraft and for the pilot(s) to implement the instruction(s). Therefore this case was selected as a suitable test case for DRM.

3 SURVEY OF POTENTIAL DRM METHODS

A variety of methods and tools for conducting DRM exist. Some methods have been in use for many years, while others are of newer date. The level of maturity of the methods varies a lot. The DRM project has identified and described a range of methods, and assessed the methods with regards to suitability for SESAR needs. In total 11 quantitative and qualitative methods have been studied. Priority has been given to methods that provide quantification of results.

The surveyed DRM methods are: Dynamic Event Trees; Dynamic Flowgraph Methodology; Discrete state-transition approaches (Markov chains, Petri Nets & extensions); Dynamic Bayesian Networks; Direct system simulation; DRM for aircraft certification; TOPAZ (Traffic Organization and Perturbation Analyzer); SoTeRia (Socio-Technical Risk Analy-

sis); FRAM (Functional Resonance Analysis Method); STPA Hazard analysis (Systems-Theoretic Process Analysis); Collision Risk Modelling; Encounter-based model methodology. For references and brief descriptions of all these methods, refer to (DRM D04 2012).

By means of an analysis against several DRM-related criteria, the DRM project has selected TOPAZ as a suitable solution for the safety risk assessment of ATM operational scenarios. TOPAZ is an agent-based DRM method that uses Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of air traffic operations up to the level of collisions. For each application, the dynamics of the agents and the time-dependent interactions within and between the agents are modelled in the syntax of Dynamically Coloured Petri Nets (DCPN) (Everdij 2010). The compositional specification by DCPNs allows for the modelling of sociotechnical systems by its broad syntax, including stochastic differential equations (e.g. describing aircraft position and velocity), discrete state transitions (e.g. describing system states or human tasks), and interactions (e.g. describing the recognition of safety-relevant conditions by humans. Detailed descriptions of TOPAZ agent-based DRM and its application to ATM operations can be accessed in Blom et al. (2001, 2006), Stroeve et al. (2009) and Eurocontrol / FAA AP15 Safety (2014).

4 APPLICATION OF DRM METHOD TO TEST CASE

The TOPAZ-based DRM method follows 10 steps which are listed below.

1. Determine the scope of operation / system for DRM
2. Get a complete/consistent description of the operation / system
3. Get a complete list of hazards
4. Develop operational hazard scenarios
5. Develop a stochastic dynamic model
6. Develop risk decomposition
7. Implement the dynamic risk model into software
8. Run Monte Carlo simulations
9. Assess bias and uncertainty
10. Develop safety risks results

The following subsections briefly describe how to apply the steps, following the initial guidance developed by the DRM project in (DRM D07 2012), and provide preliminary results on the application to the test case operation of "land vs line-up" CATC alert developed in (DRM D09 2014).

4.1 *Determine the scope of operation / system for DRM*

DRM Method: In step 1, the scope and goal of the safety assessment are identified, as well as applicable safety criteria or objectives.

Scope: The scope includes a description of the boundaries of the operation and scenarios to be modelled, the types of functions or the types of equipment/procedures/people that are included.

Goal: The goal of the risk modelling is a description of what the DRM-based safety risk assessment aims to achieve in complement to the static safety assessment results.

Safety objectives: Safety criteria or safety objectives refer to target or acceptable levels of risk that are aimed to be achieved.

Application to Test Case: The scope considers mixed mode runway operations, with aircraft landing and taking off from a single runway. The operation is considered in three cases: (1) a baseline case without CATC system, (2) a CATC-OSED case as described in Section 2, and (3) a CATC-SAR case, which is the CATC-OSED operation plus an additional requirement for the controller to enter the clearance in the CATC system before communicating it to the pilots.

The main goal of the safety study is to obtain probability estimates for three types of safety events: (a) a collision between an aircraft landing with an aircraft taxiing to the runway to line-up, (b) the taxiing aircraft entering the Instrument Landing System (ILS) sensitive area, and (c) the taxiing aircraft entering the Obstacle-Free Zone (OFZ).

4.2 *Get a complete/consistent description of the operation / system*

DRM Method: In step 2, a complete and consistent description of the operation/system under analysis is identified. This includes the operational context of the operation, the timeframe, the traffic characteristics, the geometric aspects of operation; the roles and responsibilities of the humans involved in the operation; the operational procedures, both on the ground and on board; and the logical description of the technical systems used in the operation, how they are operated and their overall performance.

Application to Test Case: Detailed information regarding operation of the system and implementation of the CATC was gathered. A short description of the CATC land versus line-up case is in Section 2.

4.3 *Get a complete list of hazards*

DRM Method: In step 3, a complete list of hazards is identified that are associated with the opera-

tion/system to be assessed. The list should include a large number and diversity of possible hazards. In addition to the Operational Hazards (identified at the level of the ATM service provided to Airspace Users) this includes hazards and conditions that may lead to a safety relevant situation (basic causes, root hazards), hazards and conditions that may hamper the resolution of the safety relevant situation (resolution hazards), and pre-existing hazards (those aviation hazards that are not caused by the ATM system but that are aimed to be prevented or mitigated by the ATM system). All the hazards identified here will be referred to in the following as 'hazards'.

Application to Test Case: The project used the material from the preceding static safety analysis, complemented by generic hazard database material from the DRM project partners, to collect a list of 42 hazards. A selection is provided below:

- Situation in which the intended trajectory of two a/c are in conflict on the Runway Protected Area.
- Failure to detect the conflicting clearances with the conflicting ATC clearances System.
- False alert of CATC system.
- Overload of pilot.
- Pilot fails to implement timely the ATCO resolution instruction following the CATC alert.

4.4 *Develop operational hazard scenarios*

DRM Method: In step 4, Operational Hazard Scenarios are constructed. Each such scenario aims to bring into account all relevant ways in which an operational hazard may develop and evolve, under influence of the related operational conditions (such as flight phase and location, level of traffic, environmental conditions), and the related hazards (i.e. basic causes, root hazards, resolution hazards, pre-existing hazards).

Application to test case: The hazards identified in the previous step have been clustered into groups of similar hazards. Next, the relations between these clusters have been depicted in the diagram shown below (ovals are hazard clusters). The clusters in the top describe hazards that may contribute to the causation of a conflict between a landing aircraft and a taxiing aircraft. The clusters in the bottom describe hazards that may hamper the recognition and resolution of the conflict via the CATC alert, the controller, and the pilots of both aircraft.

Figure 2. Operational Hazard Scenario for conflict.

4.5 *Develop a stochastic dynamic model*

DRM Method: In step 5, a multi-agent stochastic dynamic model is developed, which describes the stochastic dynamic evolution through time of one or more Operational Hazard Scenarios. The model uses the syntax of Dynamically Coloured Petri Net (DCPN) (Everdij 2010) and is developed in 6 steps:

- Step 5.1: Identify the relevant Agents
- Step 5.2: Identify the relevant entities per Agent
- Step 5.3: Specify a Local DCPN (LPN) per entity
- Step 5.4: Interconnect the LPNs within each Agent
- Step 5.5: Interconnect the Agent models
- Step 5.6: Check how the operation and each hazard has been modelled, and iterate.

Application to Test Case:
The DCPN-based model developed for the Test Case of "land vs line-up" CATC alert is too lengthy to be included in this paper; therefore, we restrict to a list of Agents and Agent entities (Table 1), and the specification of one LPN plus its inter-agent interactions.

Table 1: Description of the Agents in the DCPN-based model, and their Agent entities.

Agent	Agent Entities, plus what they model
Airport and Environment	Visibility – The visibility range
	Runway – Layout of runway
	Wind – The actual wind

Agent	Agent Entities, plus what they model
ATC System	Surveillance – Status of radar surveillance on ground and final approach
	VHF Com Runway Controller – Availability of the controller's VHF Com system
	FDP/EFS – Status of clearance input for both aircraft into the Flight Data Processing / Electronic Flight Strip system as well as status of the FDP/EFS system
	CATC Availability – Availability of CATC system
	CATC Alert – Whether CATC gives an alert
Runway controller	Situation awareness – The controller's situation awareness status and updating process, incl. position and intent of both aircraft, and awareness of CATC alerts
	Conflict action – Whether the controller gives conflict warnings to the pilots
	Clearance Specification – Status of clearance specifications by the controller to the pilots, in terms of having instructed the pilots and of having entered data into the FDP/EFS
	Workload – The current level of workload
	Skill – The level of skill of the controller
	Cognitive control mode – Whether controller is working in opportunistic or in tactical mode
Landing Aircraft	Characteristics – Aircraft type, and final approach, landing, missed approach and taxiing characteristics of the aircraft
	Evolution – Position and velocity during final approach, landing and taxiing on the runway, or during missed approach
Avionics of Landing Aircraft	VHF Com Aircraft – Availability of the VHF Com system for the landing aircraft
Pilots of Landing Aircraft	Situation Awareness – Situation awareness status and updating process of the pilots of the landing aircraft, incl. position of the own aircraft and of the taxiing aircraft, and the awareness of controller instructions
	Flight Control – The control of the aircraft by the pilots, which may be normal operation or initiation of a missed approach
Taxiing Aircraft	Characteristics – Aircraft type, taxiing and lining-up characteristics of the aircraft
	Evolution – Position and velocity during taxiing to the take-off position. As result of a conflict recognized, the aircraft may stop.
	System Boundary – Whether the taxiing aircraft is inside or outside the system boundary, i.e. the area where a conflict may occur
Avionics of Taxiing Aircraft	VHF Com Aircraft – The availability of the VHF Com system for the taxiing aircraft
Pilots of Taxiing Aircraft	Situation Awareness – Situation awareness status and updating process of the pilots of the taxiing aircraft, incl. position of the own aircraft and of the landing aircraft, and situations requiring the aircraft to stop taxiing
	Flight Control – Control of the aircraft by the pilots, which may be normal operation, or stop taxiing

The figure below presents the LPN graph for 'CATC alert', which is one of the agent entities in agent ATC System. The figure follows the syntax of DCPN, which consist of Places (circles), Transitions (squares) and Arcs (arrows) that connect the places with the transitions. The places represent the discrete modes of the entity, which in this case are *No alert* and *Alert*. At any given time, only one of these modes is the current one. A current mode holds a 'token' (not drawn below), which contains continuous valued information that further models the stochastic dynamic evolution of the model. The transitions model the switches between the modes. A switch can only be made if the transition has tokens in each of its input places, and if these tokens contain specific transition-dependent continuous-valued information.

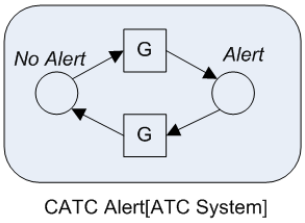

Figure 3. LPN graph for CATC Alert.

The figure below presents the input interactions (Arrows) between the LPN 'CATC Alert' and the LPNs for the entities 'CATC Availability' and 'FDP/EFS'. The transition from *No alert* to *Alert* now has three input places rather than just one, and it needs tokens in each of these input places before the switch can be made. The figure shows that the 'CATC Alert' can only switch from *No Alert* to *Alert* if the 'CATC Availability' is *Up* and the 'FDP/EFS' is *Nominal*. A second condition for this switch to occur (but not visible in the figure) is that the value of the token in place *Nominal* in LPN FDP/EFS contains the information that the landing aircraft has been given the instruction to land and the taxiing aircraft has been given the instruction to line up; this should give rise to a conflicting ATC clearance alert.

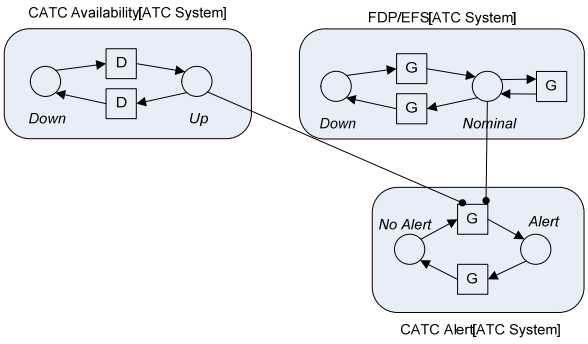

Figure 4. LPN graph for CATC Alert, plus its input interactions with CATC Availability and FDP/EFS.

The figures are further connected to other LPNs in a similar way. All figures are complemented by precise descriptions of the conditions and evolution of the LPNs and their interactions.

4.6 *Develop risk decomposition*

DRM Method: With a DCPN-based model now completed, it can next be used as basis of a Monte Carlo simulation to determine the probability of the outcome of the operational hazard, for instance an aircraft collision. To make these simulations more efficient, a risk decomposition is applied. 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. The conditional runs are started from a conditional state, which is allowed due to the specific mathematic properties of DCPN-based models (Everdij 2010).

Application to Test Case: For the test case application, the probability of occurrence of a Safety Event (such as a Collision between the landing aircraft and the taxiing aircraft) is decomposed as follows:

$$P(\textit{Safety Event}) = \sum_{k=1}^{M} P(\textit{Condition\_k}) \times P(\textit{Safety Event} \mid \textit{Condition\_k})$$

Here, the probabilities *P(Safety Event | Condition_k)* are conditional probabilities of occurrence of the safety event given a certain well-defined condition *Condition_k* that occurs at a well-defined 'stopping time', and *P(Condition_k)* is the probability of occurrence of this *Condition_k*. For the Test Case of "land vs line-up" CATC alert, the number of Conditions defined is $M = 192$, hence in the sum above, k is from 1 to 192. For example, *Condition_3* (i.e. $k = 3$) is the one where, at the stopping time: the LPN mode of the Surveillance tracking is Nominal, the LPN modes of the VHF Com for the controller and the landing aircraft are both Up, The VHF Com for the taxiing aircraft is Down, the controller intent for the taxiing aircraft is to Line-up, and the visibility condition is good.

The conditions have been chosen such that each *P(Condition_k)* can be determined analytically as a function of one or more DCPN-based model parameter values. Hence, Monte Carlo simulations are only needed to determine the *P(Safety Event | Condition_k)* for all k, after which all results are combined using the formula above. This significantly speeds up the Monte Carlo simulations by several orders of magnitude.

4.7 *Implement the dynamic risk model into software*

DRM method: In step 7, when the specification of the DCPN-based model and the risk decomposition are fully defined, they are implemented in software language in order to be able to run Monte Carlo simulations. Many software languages are suitable for this, as long as they accept all DCPN syntax principles. A major step in the software implementation is to test the code against all elements of the DCPN-based model and Risk decomposition.

Application to Test Case: The DCPN-based model and risk decomposition for "land vs line-up" CATC alert have been implemented in Delphi using Embarcadero RAD Studio XE3. It takes as input a list of model parameter values that can be set by the user, and that can be changed in order to determine risk values for various scenarios and parameter settings.

4.8 *Run Monte Carlo simulations*

DRM Method: In this step, the software implementation of the DCPN-based model is used to perform Monte Carlo simulations and compute safety risk results. Any Safety Event that can be observed in such simulation can be counted, and the number of counts, divided by the number of runs or the number of associated flight hours or movements, provides an estimate for the probability of occurrence of the Safety Event (e.g. a collision).

Application to Test Case: Risk results were produced by running a series of Monte Carlo simulations for three high-level CATC scenarios and for a set of parameters selected as being potentially representative for their impact on the safety event. Three parameter values were typically simulated in order to observe trends: a baseline value and a high and low value. At the time of writing of this paper, the application of this step was still ongoing. Some preliminary results are presented in the figures below.

In the Monte Carlo simulations the safety events defined in Step 1 were recorded: a collision between both aircraft, the taxiing aircraft entering the ILS sensitive area (150 m from the runway centerline), and the taxiing aircraft entering the OFZ (90 m from the runway centerline). The columns represent the safety event probability results for the three cases of the operation identified in Step 1: baseline without CATC, CATC-OSED, and CATC-SAR. The preliminary results indicate that the CATC system can largely reduce the collision risk, to a similar extent for the OSED and the SAR variants. The probability of entering the ILS sensitive area is hardly reduced by the CATC system. In contrast, the probability of entering the OFZ is reduced by the CATC system and notably more by the SAR variant.

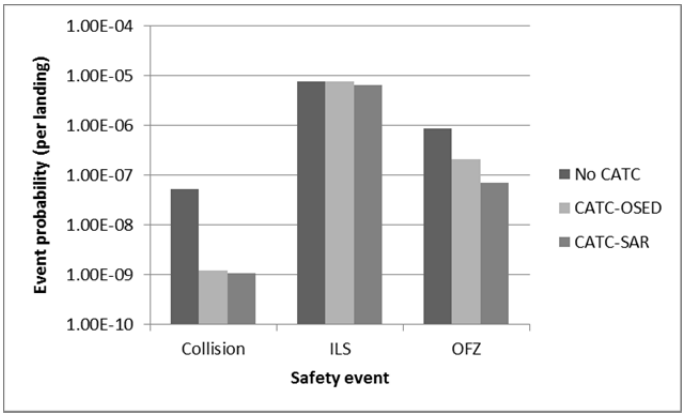

Figure 5. Event probability per landing.

The figure below shows preliminary results for the conditional probability of a collision given three visibility conditions, i.e. VC1 (good visibility), VC2 (visibility range between 400 and 2450 m), and VC3/4 (visibility range between 0 and 400 m). These results show that the conditional collision risks are higher in the poorer visibility conditions, as the controller and the pilots have less opportunity to visually detect a conflict. Furthermore, the results indicate that the CATC system is effective to a similar extent in all visibility conditions.

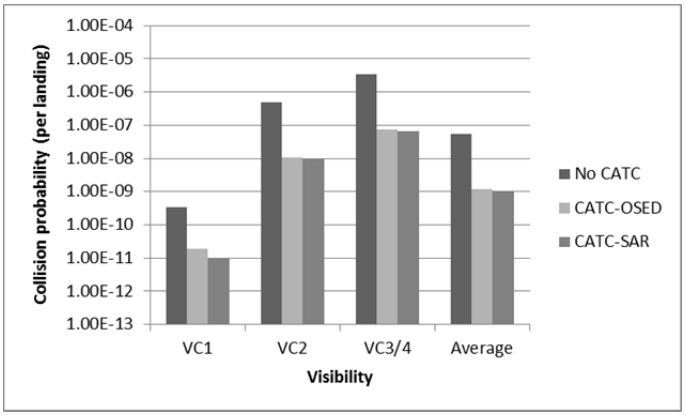

Figure 6. Collision probability per landing.

4.9 *Assess bias and uncertainty*

DRM Method: By definition, any model is not the exact image of reality. The purpose of a bias and uncertainty assessment (Everdij et al. 2006) is to identify how the differences would impact on the evaluation of the 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).

Application to Test Case: At the time of writing of this paper, the application of this step was still ongoing. The initial results showed that:

- For all of the parameters in the DCPN-based model and risk decomposition, a credibility interval could be determined. This gives insight into which parameter values are reasonably certain, and for which more data might need to be collected.
- For most of the parameters in the DCPN-based model and risk decomposition, a sensitivity assessment could be determined. A parameter has a high sensitivity if changes to its value lead to significant changes to the collision risk result. For most parameters it appeared that they have a negligible sensitivity. For some parameters the sensitivity needs to be determined in more detail using dedicated Monte Carlo simulations.

4.10 *Develop safety risks results*

DRM Method: The results of the previous steps provide point estimates and credibility intervals for the probabilities of safety events in various conditions. Comparison of these results with safety criteria provides insight in risk acceptability and risk margins. Furthermore, these results can be used to identify safety bottlenecks (aspects of the operation that contribute to unacceptable risk levels) and they provide a basis to determine safety requirements and safety objectives.

Application to Test Case: The safety risk results achieved by the DRM approach will be compared with those of the static safety assessment initially performed for the CATC operation within the SESAR project. This comparison will be used to analyse the added value of the DRM approach.

5 DISCUSSION AND CONCLUDING REMARKS

The SESAR DRM project aims to show that consideration of dynamic aspects in the safety assessment of an operation is important when studying operational concepts in which multiple operators, technical systems, the environment, and their interactions play an important role. Within the context of SESAR, Dynamic Risk Modelling (DRM) is considered to be required if the level of uncertainty in the risk results of an initial risk evaluation using a conventional (static) method is such that it cannot be conclusively argued whether the risk is acceptable or not. In addition, at least one of the following criteria needs to hold true: a) The system behaviour, when considering equipment functional variability, failures, human performance variability and errors, in-

volves occurrences which cannot be considered in isolation, as they strongly depend on system status over time. b) The system behaviour when considering equipment functional variability, failures, human performance variability and errors depends on process variables.

By means of an analysis against several DRM-related criteria, the DRM project has selected TOPAZ from a list of candidate DRM methods as a suitable solution for the safety risk assessment of ATM operational scenarios. TOPAZ is an agent-based DRM method that uses Monte Carlo simulations and uncertainty evaluations to analyse the safety risk of air traffic operations up to the level of collisions. The project produced guidelines for the application of this method in SESAR context, and applied the method to a SESAR Test Case of "Land vs Line-up" Conflicting ATC Clearances.

The Test Case has shown that DRM is able to model the stochastic dynamic aspects of an operation with more accuracy than is possible with static methods. Examples are the position and velocity of aircraft as they evolve through time, the stochastic dynamic behaviour of human operators in response to their environment, situation awareness differences between various actors, multiple scenarios that unfold under influence of hazards occurring, environmental changes, events occurring earlier or later than average, etc.

The preliminary DRM-based risk results show interesting differences with those of the preceding static safety assessment, which will be systematically studied in the remainder of the DRM project.

Acknowledgements and Disclaimer

The work presented in this paper is financed by the SESAR Joint Undertaking (SESAR JU) programme. NLR contributes to the SESAR project on behalf of DFS Deutsche Flugsicherung GmbH. The authors thank project members AIRBUS (especially Joelle Monso, Eric Hannouz, Lionel Marie-Magdeleine), DFS (especially Viktoria Weigel), ENAV (especially Tiziana Russo) and SELEX (especially Angela Errico) for their contributions. This paper presents the authors' view only and is not intended to represent organizations or the SESAR JU position.

References

Averty, P., Mehadhebi, K., Pirat, J.L. 2009. Evaluation of ATC working practice from a safety and human factor perpective. Eight USA/Europe Air Traffic Management and Research Seminar.

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

Blom, H.A.P., Stroeve, S.H., & De Jong, H.H. (2006). Safety risk assessment by Monte Carlo simulation of complex safety critical operations. In F. Redmill & T. Anderson (Eds.), Developments in Risk-based Approaches to Safety: Proceedings of the Fourteenth Safety-critical Systems Symposium, Bristol, U.K., 7-9 February 2006: Springer.

DRM D04. (2012). SESAR P16.01.03 Deliverable D04: Identification of Dynamic Risk Modelling for SESAR needs, Selection of DRM solution for SESAR.

DRM D07. (2012). SESAR P16.01.03 Deliverable D07: Initial guidelines for Dynamic Risk Modelling (DRM) application.

DRM D09. (2014). SESAR P16.01.03 Deliverable D09: Dynamic Risk Modelling (DRM) Test Case application.

Eurocontrol / FAA AP15 Safety. (2014). Agent-based dynamic risk modelling for ATM: A white paper.

Eurocontrol (2009). 'Feasibility study on Dynamic Risk Modelling for ATM Applications', by M.H.C. Everdij, S.H. Stroeve.

Everdij, M.H.C., Blom, H.A.P., & Stroeve, S.H. (2006). Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management, New Orleans, USA.

Everdij, M.H.C. (2010). Compositional modelling using Petri nets with the analysis power of stochastic hybrid processes. PhD. Thesis, University of Twente. http://www.nlr-atsi.nl/eCache/ATS/15/060.pdf.

Herrera, et al. 2011. DRM project – Develop Techniques for Dynamic Risk Modelling. SESAR P16.01.03. Project Initiation report.

SESAR SRM. (2012). SESAR WP 16.06.01 Deliverable D06: SESAR Safety Reference Material, version 00-02-02.

SAR CATC. (2012). Safety Assessment Report for Conflicting ATC clearances SESAR P06.07.01, D17B, ed00.01.03 09/08/2012.

Stroeve, S.H., Blom, H.A.P., & Bakker, G.J. (2009). Systemic accident risk assessment in air traffic by Monte Carlo simulation. Safety Science, 47 (2), 238-249. doi:10.1016/j.ssci. 2008. 04.003