

Nationaal Lucht- en Ruimtevaartlaboratorium

National Aerospace Laboratory NLR



NLR-TP-2006-290

Free flight safety risk modelling and simulation

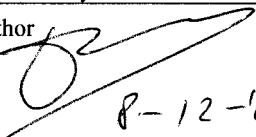
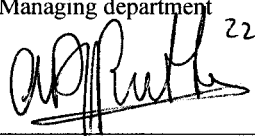
H.A.P. Blom, G.J. Bakker, B. Klein Obbink and M.B. Klompstra

This report contains a paper presented at 2nd International Conference on Research in Air Transportation ICRAAT 2006, at Beograd, Serbia, June 24-28, 2006.

This report may be cited on condition that full credit is given to NLR and the authors

Customer: National Aerospace Laboratory NLR
Working Plan number: 2005 AT.1.A
Owner: National Aerospace Laboratory NLR
Division: Air Transport
Distribution: Unlimited
Classification title: Unclassified
September 2006

Approved by:

Author  8-12-'06	Reviewer Anonymous peer reviewers	Managing department  22/12/06
---	--------------------------------------	--

Free flight safety risk modeling and simulation

Henk A.P. Blom, G.J. (Bert) Bakker, Bart Klein Obbink and Margriet B. Klompstra

Abstract— The basic notion of free flight is that aircrews obtain the freedom to select their trajectory including the responsibility of resolving conflicts with other aircraft. Under low en-route traffic loads there is general agreement that free flight can be safely applied. Under increasing traffic loads, however, the answer to this question becomes unknown. Free flight would change ATM in such a fundamental way, that one can speak of a paradigm shift and that comes with emerging behavior, i.e. novel behavior which is exhibited at the system-wide level and emerges from the combined dynamical actions and reactions by individual systems and humans that affect the operations. Because emerging behavior cannot be predicted from previous experience, we need a complementary approach in estimating the safety of free flight under relatively high traffic levels. This paper explains how recently developed methods in Petri net specification and sequential Monte Carlo simulation can be used to make progress in addressing this outstanding issue. The paper also presents the results of an initial application of these novel methods to a well developed autonomous free flight concept of operations.

Index Terms—Sequential Monte Carlo simulation, Petri net modelling, Safety risk assessment, Safety-critical systems, Autonomous Free flight

I. INTRODUCTION

TECHNOLOGY allows aircraft to broadcast information about the own-ship position and velocity to surrounding aircraft, and to receive similar information from surrounding aircraft. This development has stimulated the rethinking of the overall concept for today's Air Traffic Management (ATM), e.g. to transfer responsibility for conflict prevention from ground to air. As the aircrews thus obtain the freedom to select their trajectory, this conceptual idea has been called Free Flight [1]. It changes ATM in such a fundamental way, that one could speak of a paradigm shift: the centralised control becomes a distributed one, responsibilities transfer from ground to air, fixed air traffic routes are removed and appropriate new technologies are brought in. In free flight, each individual aircrew has the responsibility to timely detect and solve conflicts, thereby assisted by navigation means, surveillance processing and equipment displaying conflict-solving trajectories. Due to the potentially many aircraft

involved, the system is highly distributed. This free flight concept definition leaves open many challenges in developing adequate procedures, algorithms, equipment performance requirements, and has motivated the study of multiple Free Flight operational concepts, implementation choices and requirements, e.g. [2]-[6]. Crucial in this process is to learn understanding how to optimize free flight designs for safety and capacity [7].

The aim of this paper is to study the safety risk assessment of en-route free flight operations through modeling and Monte Carlo simulation. In [8], such a study has been performed for free flight equipped aircraft that are obliged to remain flying within a conventional fixed route structure. The current paper, however, studies a true free flight concept of operations, i.e. one without using fixed route structure. The free flight concept we identified for this has been developed for air traffic in the Mediterranean area [9]. For short we refer to this operational concept as Autonomous Mediterranean Free Flight (AMFF). We illustrate an advanced model specification and sequential MC simulation approach towards the assessment of collision risk of AMFF operation under relatively high traffic density.

For advanced air traffic operations, [10] gives a nice illustration how statistical data in combination with a fault tree of the functionalities of the advanced operation can serve to predict how reliability of free flight supported systems impact contributions to collision risk of an advanced operation [11]. Through an example it is shown how this allows improvement of the design, such that the reliability-implied contribution to collision risk can be lowered to a desired value.

Also following a fault tree approach, the safety of the AMFF concept of operations has been assessed [12], including real-time simulations of non-nominal conditions [13]-[15]. The results obtained show that application of AMFF seems feasible for accommodating low en-route traffic conditions over the Mediterranean. In order to assess whether AMFF can safely accommodate higher traffic levels, [12] recommends to use a more advanced safety risk assessment approach that considers complex situations involving dynamic interactions between multiple human actors and other systems.

The recommendation by [12] concurs well with the explanation by [16] that the key difficulty of evaluating advanced operations is to include emergent behavior, i.e. novel behavior which is exhibited at the system-wide level and emerges from the combined dynamical actions and reactions by individual systems and humans within the system. This emergent behavior typically cannot be foreseen and evaluated by examining the individuals' behavior alone. In [16] it is

Manuscript received February 26, 2006 and revised April 26, 2006. This work was supported through the European Commission project HYBRIDGE, IST-2001-32460.

Henk Blom, Bert Bakker, Bart Klein Obbink and Margriet Klompstra are with National Aerospace Laboratory NLR, Amsterdam, The Netherlands, blom@nlr.nl; bakker@nlr.nl; bklein@nlr.nl and klompstr@nlr.nl.



explained that agent based simulation allows to predict the impact of revolutionary changes in air transportation; it integrates cognitive models of technology behavior and description of their operating environment. Simulation of these individual models acting together can predict the results of completely new transformations in procedures and technology. Their MC simulations reach up to the level of novel emerging hazardous events. For safety risk assessment however, it is required to go further with the MC simulations up to the level of emerging catastrophic events. In en-route air traffic these catastrophic events are mid-air collisions. The approach described in this paper is an example of the latter approach to estimate such a difficult metric of collision risk between aircraft by the use of advanced approaches in Petri Net modeling and Monte Carlo simulation.

The paper is organized as follows. Section II provides a brief overview of the AMFF concept of operations selected for evaluation on collision risk and explains how this operational concept has been modeled in a specific Petri net formalism. Section III explains the sequential Monte Carlo simulation acceleration approach developed for assessing collision risk for the AMFF simulation model. Section IV presents results of Monte Carlo simulations performed for three AMFF scenarios. Section V discusses the results obtained.

II. DEVELOPMENT OF PETRI NET MODEL OF AMFF

For the development of a Petri net model of an advanced operation, two key challenges have to be addressed: a syntactical challenge of developing a model that is consistent, complete and unambiguous, and a semantics challenge of developing appropriate human cognition performance models. This section explains how the syntactical challenge has been addressed. For the mechanism to manage the semantics challenge, we have followed the approach studied and developed in, e.g. [17]-[21]. The explanation of how this cognitive human performance modeling approach has been applied to AMFF falls outside the current paper's scope.

A. AMFF operation

For a complete description of the AMFF operational concept we refer to [9], [14]. In addition, [22] describes the background of the AMFF design philosophy. A practical implication was to avoid much information exchange between aircraft and to avoid dedicated decision-making by artificial intelligent machines. Although the conflict detection and resolution approach developed for AMFF has its roots in the modified potential field approach [4], there are significant differences. The main difference is that conflict resolution in AMFF is intentionally designed not to take the potential field of all aircraft into account. The resulting AMFF design can be summarized as follows:

- All aircraft are supposed to be equipped with Automatic Dependent Surveillance-Broadcast (ADS-B), which is a system that periodically broadcasts own aircraft state information, and continuously receives

the state information messages broadcasted by aircraft that fly within broadcasting range (~ 100 NM).

- In order to comply to pilot preferences, conflict resolution algorithms are designed to solve multiple conflicts one by one rather than according to a full concurrent way that can be handled by the modified potential field approach [4].
- Conflict detection and resolution are state-based, that is: intent information, such as information at which point surrounding aircraft will change course or height, is supposed to be unknown.
- The vertical separation minimum is 1000 ft and the horizontal separation minimum is 5 Nm. A conflict is detected if these separation minima will be violated within 6 minutes.
- The conflict resolution process consists of two phases. During the first phase, one of the aircraft crews should make a resolution maneuver. If this does not work, then during the second phase, both crews should make a resolution maneuver.
- Prior to the first phase, the crew is warned when an ASAS alert is expected to occur if no preventive action would be timely implemented; this prediction is done by a system referred to as P-ASAS (Predictive ASAS).
- Conflict co-ordination does not take place explicitly, i.e. there is no communication on when and how a resolution maneuver will be executed.
- All aircraft are supposed to use the same resolution algorithm, and all crew are assumed to use ASAS and to collaborate in line with the procedures.
- Two conflict resolution maneuver options are presented: one in vertical and one in horizontal direction. The pilot decides which option to execute.
- ASAS related information is presented to the crew through a Cockpit Display of Traffic Information (CDTI).

B. Stochastically and Dynamically Coloured Petri Net

The most advanced approaches that have been developed in literature to model accident risk of safety-critical operations in nuclear and chemical industries make use of the compositional specification power of Petri nets to instantiate a model, and subsequently use stochastic analysis and Monte Carlo simulation (e.g. [23]) to evaluate the model. Since their introduction in the 1960s, Petri nets have shown their usefulness for many practical applications in different industries (e.g. [24]). Various Petri net extensions and generalisations, new analysis techniques, and numerous supporting computer tools have been developed, which further increased their modelling opportunities, though falling short for air traffic operations. In order to capture the characteristics of air traffic operations through a Petri net, [25]-[27] introduced Dynamically Coloured Petri Net (DCPN) and



Stochastically and Dynamically Coloured Petri Net (SDCPN), and proved that there exists a one-to-one relation with the larger class of stochastic processes and analysis techniques needed for air traffic operations [28].

A Coloured PN is a Petri net with a colour attached to each token. Such a colour assumes values from a given set, and this value does not change as long as the token stays in its place. When a token is “transferred” from one place to another place, then the colour moves with the token to the next place and may also be updated. In a DCPN a colour value may evolve as the solution of an ordinary differential equation (ODE). In a SDPCPN a colour value may evolve as the solution of a stochastic differential equation (SDE).

The specification of an SDPCPN for a complex process or operation is accomplished in a compositional way [29]. It starts with developing relevant Local Petri Nets (LPNs) for each agent that exists in the process or operation (e.g. air traffic controller, pilot, navigation and surveillance equipment). Essential is that these LPNs are allowed to be connected with other Petri net parts in such a way that the number of tokens residing in an LPN is not influenced by these interconnections. We use two types of basic interconnection arcs between nodes and arcs in different LPNs:

- Enabling arc (or inhibitor arc) from one place in one LPN to one transition in another LPN. These types of arcs have been used widely in Petri net literature.
- Interaction Petri Net (IPN) from one (or more) transition(s) in one LPN to one (or more) transition(s) in another LPN.

In addition, a box is drawn around each LPN, and hierarchical interconnection arcs from or to an edge of an LPN box are defined to represent several arcs or transitions by only one arc or transition.

C. Agents and LPNs to represent AMFF operations

In the Petri Net modeling of AMFF operations for the purpose of an initial collision risk assessment, the following agents are taken into account:

- Aircraft
- Pilot-Flying (PF)
- Pilot-Not-Flying (PNF)
- Airborne Guidance, Navigation and Control
- Airborne Separation Assistance System (ASAS)
- Communication / Navigation / Surveillance

It should be noticed that our initial model does not yet incorporate Airborne Collision Avoidance System (ACAS), Airline Operations Centre (AOC), Air Traffic Control (ATC) and an environmental model.

Per agent, particular LPNs and IPNs have been developed and subsequently the interactions between these LPNs and IPNs have been specified. The listing of agents and LPNs is:

- Aircraft LPNs:
 - Type
 - Evolution mode
 - Systems mode

- Emergency mode
- Pilot-Flying (PF) LPNs:
 - State Situation Awareness
 - Intent Situation Awareness
 - Goal memory
 - Current goal
 - Task performance
 - Cognitive mode
- Pilot-Not-Flying (PNF) LPNs:
 - Current goal
 - Task performance
- ASAS LPNs:
 - Processing
 - Alerting
 - Audio alerting
 - Surveillance
 - System mode
 - Priority switch mode
 - Anti-priority switch mode
 - Predictive alerting (of other aircraft)
- Airborne GNC (Guidance, Navigation, Control) LPNs:
 - Indicators failure mode for PF
 - Engine failure mode for PF
 - Navigation failure indicator for PF
 - ASAS failure indicator for PF
 - ADS-B receiver failure indicator for PF
 - ADS-B transmitter failure indicator for PF
 - Indicator failure mode for PNF
 - Guidance mode
 - Horizontal guidance configuration mode
 - Vertical guidance configuration mode
 - FMS flightplan
 - Airborne GPS receiver
 - Airborne Inertial Reference System (IRS)
 - Altimeter
 - Horizontal position processing
 - Vertical position processing
 - ADS-B transmission
 - ADS-B receiver
- Communication / Navigation / Surveillance LPNs:
 - Global GPS / satellites
 - Global ADS-B ether frequency
 - SSR Mode-S frequency

The actual number of LPNs in the whole model then equals $38N+3$, where N is the number of aircraft. In addition the number of IPNs equals $35N$.

D. Interconnected LPNs of ASAS

ASAS is modeled through the SDPCPN depicted in Figure 1. The ADS-B information received from other aircraft is processed by the *LPN ASAS surveillance*. Together with the information about its own aircraft state information (from AGNC), the *LPN ASAS processing* uses this information to perform conflict detection and resolution functionalities. Subsequently, the *LPN ASAS alerting* and the *LPN P-ASAS alerting* informs the PF and PNF through *ASAS audio alerting* about any aircraft that is in potential ASAS conflict with the

own aircraft, and suggests resolution options including a prioritization. Three complementary LPNs represent non-nominal behavior modes, each combination of which has a specific influence on the ASAS alerting LPN:

- ASAS system mode may be working, failed or corrupted (failed or corrupted mode also influences the ASAS processing LPN).
- ASAS priority switching mode; under emergency, the PF switches this from “off” to “on”.
- ASAS anti-priority switch; this is switched from “off” to “on” when own ADS-B is not working.

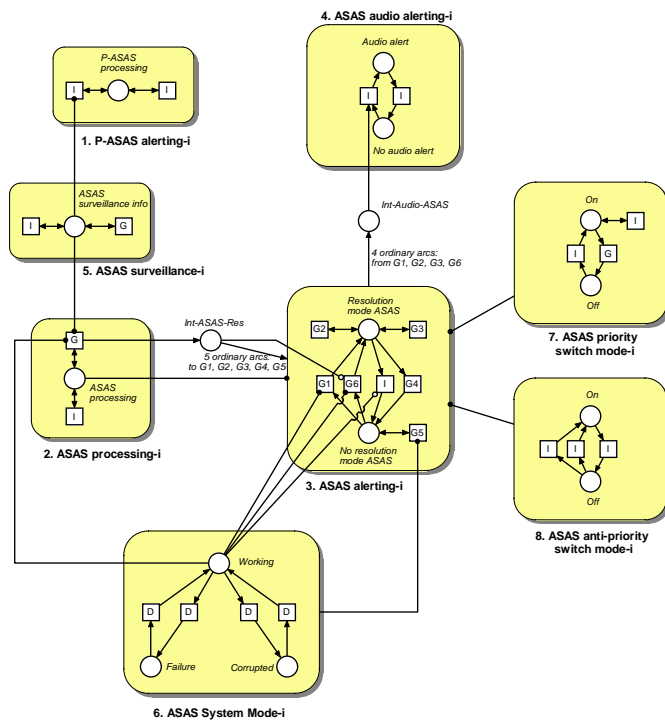


Figure 1. The agent ASAS in AMFF is modelled by eight LPNs, a number of ordinary and enabling arcs and two IPNs (with one place each).

E. Interconnected LPNs of Pilot Flying

This subsection illustrates the specific Petri Net model developed for the Pilot Flying. A graphical representation of all LPNs the Pilot-Flying consists of, is given in Figure 2. The Human-Machine-Interface where sound or visual clues might indicate that attention should be paid to a particular issue, is represented by an IPN that is not depicted in the Figure. Similarly, the arcs to or from any other agent are not shown in Figure 2. Because of the very nature of Petri Nets, these arcs can easily be added during the follow-up specification cycle. To get an understanding of the different LPNs, a good starting point might be the LPN “Current Goal” (at the bottom of the figure) as it represents the objective the Pilot-Flying is currently working on. Examples of such goals are “Collision Avoidance”, “Conflict Resolution” and “Horizontal

Navigation”. For each of these goals, the pilot executes a number of tasks in a prescribed or conditional order, represented in the LPN “Task Performance”. Examples of such tasks are “Monitoring and Decision”, “Execution” and “Execution Monitoring”. If all relevant tasks for the current goal are considered executed, the pilot chooses another goal, thereby using his memory (where goals deserving attention might be stored, represented by the LPN “Goal Memory”) and the Human-Machine-Interface. His memory where goals deserving attention might be stored is represented as the LPN “Goal Memory” in Figure 2.

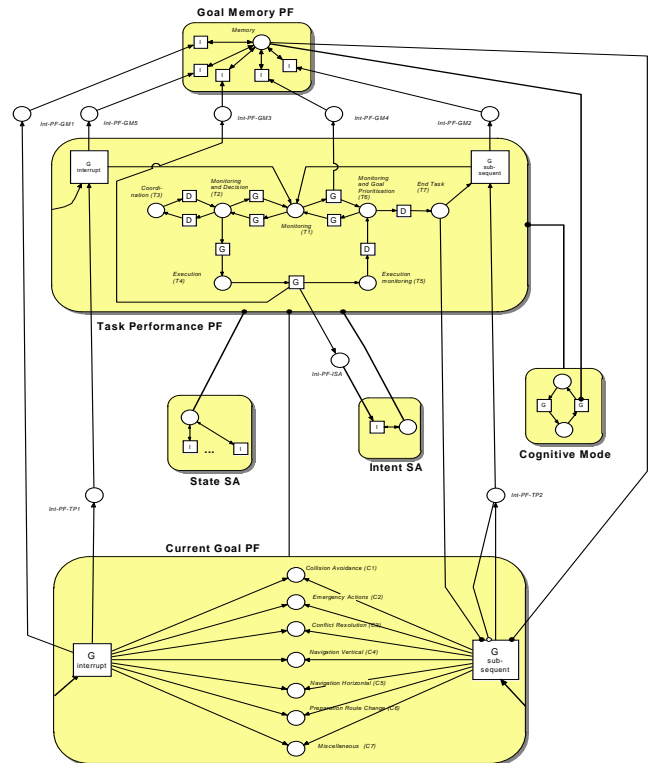


Figure 2. The agent Pilot-Flying in AMFF is modelled by six LPNs, and a number of ordinary and enabling arcs, and some IPNs, consisting of one place and input and output arcs.

So, the LPNs “Current Goal”, “Task Performance”, and “Goal Memory” are important in the modelling of which task the Pilot-Flying is executing. The other three LPNs are important in the modelling on how the Pilot-Flying is executing the tasks. The LPN “State SA”, where SA stands for Situation Awareness, represents the relevant perception of the pilot about the states of elements in his environment, e.g. whether he is aware of an engine failure. The LPN “Intent SA” represents the intent, e.g. whether he intends to leave the Free Flight Airspace. The LPN “Cognitive mode” represents whether the pilot is in an opportunistic mode, leading to a high but error-prone throughput, or in a tactical mode, leading to a moderate throughput with a low error probability.

F. Model parametrization, verification and validation

The compositionally specified SDCPN model enables a systematic implementation, verification and validation of the resulting Monte Carlo simulator. This is done through the following systematic steps:

- Software code testing. This is done through conducting the following sequence of testing: random number generation, statistical distributions, common functions, each LPN implementation, each agent implementation, interactions between all agents, full MC simulation;
- Numerical approximation testing. This is needed to identify maximally allowable numerical integration step and minimally required number of particular MC simulations;
- Graphical user interface testing. This is to verify that the input and output of data works well;
- Parameterization. This is done through a search for literature and statistical sources, and complemented by expert interviews. The fusion of these different pieces of information is accomplished following a Bayesian approach;
- Initial model validation through studying MC simulator behavior and sensitivities to parameter changes under dedicated scenarios;
- Overall validation, which is directed to the evaluation of differences between model and reality and what effect these differences have at the assessed risk level [30], [31]. Statistical data collection and analysis, and active participation of operational experts is required.

The last step should start as early as possible, but should also continue throughout the operational concept development cycles. Typically, this way of working allows a significant improvement of the validation level of the simulation model per concept development and safety risk assessment cycle.

III. MONTE CARLO SIMULATION OF COLLISION RISK

The basic idea of assessing collision risk is to perform many Monte Carlo simulations with the SDCPN model, and while doing so, to estimate the collision risk by counting the number of collisions and dividing this by the number of simulated flight hours. Though this idea is simple, in order to make it work in practice, we need an effective way of speeding up the Monte Carlo simulation. This section describes the way we are doing this by extending the sequential MC simulation approach of [32], [33] to collision risk in air traffic.

A. Simulation to first moment of collision

In [27] it has been shown that an SDCPN model represents a stochastic differential equation (SDE) on a hybrid state space, driven by Brownian motion and Poisson random measure. In [34] it has been shown that under reasonable conditions (typically also adopted when specifying an SDCPN) the solution of this SDE is a strongly unique stochastic hybrid process $\{x, \theta\}$ which has mathematically properties that enable powerful stochastic analysis

(semimartingale and strong Markov). In view of this, [35] has extended the approach of [32] to these stochastic hybrid processes. This allows us to study the speeding up of the AMFF simulation in this general setting, and avoids a need to dive into all kind of details of the AMFF model.

For the N -aircraft traffic scenario the process $\{x, \theta\}$ consists of components $x_t \triangleq \text{Col}\{x_t^0, x_t^1, \dots, x_t^N\}$ and $\theta_t \triangleq \text{Col}\{\theta_t^0, \theta_t^1, \dots, \theta_t^N\}$, x_t^i assumes values from \mathbb{R}^{n_i} , and θ_t^i assumes values from a finite set (M^i) . $\{x_t^i, \theta_t^i\}$, $i=1, \dots, N$, is the hybrid state process related to the i -th aircraft, and $\{x_t^0, \theta_t^0\}$ is the non-aircraft related hybrid state process. The total process $\{x, \theta\}$ is $\mathbb{R}^n \times M$ -valued with

$$n = \sum_{i=0}^N n_i \text{ and } M = \otimes_{i=0}^N M_i.$$

In order to model collisions between aircraft, we introduce mappings from the Euclidean valued process $\{x_t\}$ into the relative position and velocity between a pair of aircraft (i, j) . The relative horizontal and vertical positions are obtained through the mappings $y^{ij}(x_t)$ and $z^{ij}(x_t)$ respectively. The relative horizontal velocity and the vertical rate of climb/descent are obtained through the mappings $v^{ij}(x_t)$ and $r^{ij}(x_t)$ respectively. The relations between these position and velocity mappings satisfy:

$$dy^{ij}(x_t) = v^{ij}(x_t) dt \quad (1)$$

$$dz^{ij}(x_t) = r^{ij}(x_t) dt \quad (2)$$

A collision between aircraft (i, j) means that the process $\{y^{ij}(x_t), z^{ij}(x_t)\}$ hits the boundary of an area where the distance between aircraft i and j is smaller than their physical size. Under the assumption that the length of an aircraft equals the width of an aircraft, and that the volume of an aircraft is represented by a cylinder the orientation of which does not change in time, then aircraft (i, j) have zero separation if $x_t \in D^{ij}$ with:

$$D^{ij} = \{x \in \mathbb{R}^n; |y^{ij}(x)| \leq (l_i + l_j)/2 \text{ AND } |z^{ij}(x)| \leq (s_i + s_j)/2\}, i \neq j \quad (3)$$

where l_j and s_j are length and height of aircraft j . For simplicity we assume that all aircraft have the same size, by which (3) becomes:

$$D^{ij} = \{x \in \mathbb{R}^n; |y^{ij}(x)| \leq l \text{ AND } |z^{ij}(x)| \leq s\}, i \neq j \quad (4)$$

Notice that in (4), D^{ij} depends of (i, j) .



If x_t hits D^{ij} at time τ^{ij} , then we say a collision event between aircraft (i,j) occurs at moment τ^{ij} , i.e.

$$\tau^{ij} = \inf\{t > 0; x_t \in D^{ij}\}, \quad i \neq j \quad (5)$$

Next we define the first moment τ^i of collision with any of the other aircraft, i.e.

$$\begin{aligned} \tau^i &= \inf_{j \neq i} \{\tau^{ij}\} = \inf_{j \neq i} \{t > 0; x_t \in D^{ij}\} \\ &= \inf\{t > 0; x_t \in D^i\} \end{aligned} \quad (6)$$

with $D^i = \bigcup_{j \neq i} D^{ij}$. At moment τ^i we can stop the simulation of the process $\{x_t^i, \theta_t^i\}$.

An unbiased estimation procedure of the probability $\mathbb{P}(\tau_m^i < T)$ of collision on $[0, T]$ would be to simulate many times aircraft i amidst other aircraft over a period of length T and count all cases in which the realization of the moment τ^i is smaller than T . An estimator for the collision risk of aircraft i per unit T of time then is the fraction of simulations for which $\tau^i < T$.

B. Risk factorization using multiple conflict levels

Prior to a collision of aircraft i with aircraft j a sequence of conflicts ranging from long term to short term always occurs. In order to incorporate this explicitly in the MC simulation, we formalize this sequence of conflict levels through the sequence of closed subsets of \mathbb{R}^n , $D^{ij} = D_m^{ij} \subset D_{m-1}^{ij} \subset \dots \subset D_1^{ij}$, with for $k = 1, \dots, m$:

$$\begin{aligned} D_k^{ij} &= \{x \in \mathbb{R}^n; |y^{ij}(x) + \Delta v^{ij}(x)| \leq d_k \text{ AND} \\ &|z^{ij}(x) + \Delta r^{ij}(x)| \leq h_k, \text{ for some } \Delta \in [0, T_k]\}, \quad i \neq j \end{aligned} \quad (7)$$

where d_k , h_k and T_k are the parameters of the conflict definition at level k , and with $d_m = l$, $h_m = s$ and $T_m = 0$, and with $d_{k+1} \geq d_k$, $h_{k+1} \geq h_k$ and $T_{k+1} \geq T_k$. If x_t hits D_k^{ij} at time τ_k^{ij} , then we say the first level k conflict event between aircraft (i,j) occurs at moment τ_k^{ij} , i.e.

$$\tau_k^{ij} = \inf\{t > 0; x_t \in D_k^{ij}\} \quad (8)$$

Similarly as we did for the collision level, for aircraft i we consider the first moment τ_k^i that aircraft i reaches conflict level k with any of the other aircraft, i.e.

$$\begin{aligned} \tau_k^i &= \inf_{j \neq i} \{\tau_k^{ij}\} = \inf_{j \neq i} \{t > 0; x_t \in D_k^{ij}\} \\ &= \inf\{t > 0; x_t \in D_k^i\} \end{aligned} \quad (9)$$

with $D_k^i \triangleq \bigcup_{j \neq i} D_k^{ij}$.

Following [35], we can write the probability of collision of aircraft i with any of the other aircraft as a product of conditional probabilities of reaching the next conflict level given the current conflict level has been reached:

$$\mathbb{P}(\tau_m^i < T) = \prod_{k=1}^m \gamma_k^i \quad (10)$$

where $\gamma_k^i \triangleq \mathbb{P}(\tau_k^i < T | \tau_{k-1}^i < T)$

With this, the problem can be seen as one to estimate the conditional probabilities γ_k^i in such a way that the product of these estimators is unbiased. Let $\bar{\gamma}_k^i$ denote the value estimated for γ_k^i . Because of the multiplication of the various individual $\bar{\gamma}_k^i$ estimated values, which depend on each other, in general such a product may be heavily biased. The key novelty of [32] was to show that such a product may be evaluated in an unbiased way when $\{x_t\}$ makes part of a larger stochastic process that satisfies the strong Markov property. Hence the resulting sequential MC simulation essentially consists of taking advantage of the nested sequence of closed subsets of \mathbb{R}^n : $D = D_m^i \subset D_{m-1}^i \subset \dots \subset D_1^i$, and then start simulation from outside D_1^i to D_1^i (this yields $\bar{\gamma}_1^i$), and subsequently simulate from D_1^i to D_2^i (this yields $\bar{\gamma}_2^i$), from D_2^i to D_3^i (this yields $\bar{\gamma}_3^i$), ..., and finally from D_{m-1}^i to D_m^i (this yields $\bar{\gamma}_m^i$). The estimated risk for aircraft i to collide with any of the other aircraft then is $\prod_{k=1}^m \bar{\gamma}_k^i$.

IV. SIMULATED SCENARIOS AND COLLISION RISK ESTIMATES

The sequential MC simulation approach outlined in section III is now applied to three hypothetical AMFF scenarios. The first scenario has eight aircraft that fly at the same flight level. Based on their flight plans, the eight aircraft are expect to fly through the same point in space at the same moment in time. The second scenario has one aircraft flying through an area of seven randomly distributed aircraft per container of 40 Nm x 40 Nm x 3000 feet. The third scenario is the same as the second, except with a container that is twice as large in width/length. Prior to describing these scenarios and simulation results, we explain the parametrization of the IPS algorithm used.

A. Parameterization of the IPS simulations

The main safety critical parameter settings of the AMFF enabling technical systems (GPS, ADS-B and ASAS) are given in the Table I.

TABLE I. PARAMETER VALUES OF AMFF ENABLING TECHNICAL SYSTEMS

Model Parameter	Probability
Global GPS down	1.0×10^{-5}
Global ADS-B down ¹	1.0×10^{-6}
Aircraft ADS-B Receiver down	5.0×10^{-5}
Aircraft ADS-B Transmitter down	5.0×10^{-5}
Aircraft ASAS System mode corrupted	5.0×10^{-5}
Aircraft ASAS System mode failure	5.0×10^{-5}

The IPS conflict levels k are defined by parameter values for lateral conflict distance d_k , conflict height h_k and time to conflict T_k . These values have been determined through two steps. The first was to let an operational expert make a best guess of proper parameter values. Next, during initial simulations with the IPS some fine tuning of the number of levels and of parameter values per level has been done. The resulting values are given in Table II.

TABLE II. IPS CONFLICT LEVEL PARAMETER VALUES

k	1	2	3	4	5	6	7	8
d_k (Nm)	4.5	4.5	4.5	4.5	2.5	1.25	0.5	0.054
h_k (ft)	900	900	900	900	900	500	250	131
T_k (min)	8	2.5	1.5	0	0	0	0	0

B. Eight aircraft on collision course

In this simulation eight aircraft start at the same flight level, some 250 km out of each other, and fly in eight 45 degrees differing directions with a ground speed of 240 m/s, all up to the same point in the middle. By running ten times the IPS algorithm the collision risk is estimated ten times. The number of particles per IPS simulation run is 12,000. The total simulation time took about 20 hours on two machines, and the computer memory load was about 2.0 GigaByte per machine.

For the first four IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table III for each of the conflict levels, $k = 1, \dots, 8$, and aircraft $i = 1$. It can be seen that the first IPS run has zero particles that reach the last (8th level). Hence the first IPS run does not yield a useful estimate, and is not used for estimating the risk.

¹ Global ADS-B down refers to frequency congestion/overload of the data transfer technology used for ADS-B.

TABLE III. FRACTIONS COUNTED DURING FOUR IPS RUNS OF SCENARIO 1

Level	1 st IPS	2 nd IPS	3 rd IPS	4 th IPS
1	1.000	1.000	1.000	1.000
2	0.528	0.529	0.539	0.533
3	0.426	0.429	0.424	0.431
4	0.033	0.036	0.035	0.037
5	0.175	0.180	0.183	0.181
6	0.267	0.158	0.177	0.144
7	0.150	0.268	0.281	0.427
8	0.000	0.009	0.233	0.043
Product of fractions	0.0	5.58×10^{-7}	1.67×10^{-5}	4.01×10^{-6}

The IPS estimated mean probability for one aircraft to collide with any of the other seven aircraft equals 2.2×10^{-5} . The minimum and maximum values now are respectively a factor 250 lower and a factor 4 higher than the mean value. We also verified that this risk value was not sensitive at all to the failure rates of the ASAS related technical systems.

In [4] a similar eight aircraft encounter scenario had been simulated many times, without experiencing any collision event. However, at a collision probability value of 2.2×10^{-5} , one needs to run about 6,000 runs to have a 50% chance of counting at least one collision, and this high number of independent simulations with the eight aircraft encounter have not been performed. As such the current results agree quite well with the fact that in these earlier simulations for the eight aircraft scenario no collision has been observed. We also verified that the novel simulation results for the eight aircraft scenario agreed quite well with the expectation of the designers of the AMFF operational concept.

C. Free flight through an artificially constructed airspace

In this simulation the complete airspace is divided into packed containers. Within each container a fixed number of seven aircraft ($i=2, \dots, 8$) fly at arbitrary position and in arbitrary direction at a ground speed of 240 m/s. One additional aircraft ($i=1$) aims to fly straight through a sequence of connected containers, at the same speed, and the aim is to estimate its probability of collision with any of the other aircraft per unit time of flying.

Per container, the aircraft within it behave the same. This means that we have to simulate each aircraft in one container only, as long as we apply the ASAS conflict prediction and resolution also to aircraft copies in the neighboring containers. In principle this can mean that an aircraft experiences a conflict with its own copy in a neighboring container. This also means that the size of a container should not go below a certain minimum size.

By changing container size we can vary traffic density. To choose the appropriate traffic density, our reference point is the highest number (17) of aircraft counted at 23rd July 1999 in an en-route area near Frankfurt of size 1 degree x 1 degree x FL290-FL420. This comes down to 0.0032 a/c per Nm³. For our simulation we assume a 3 times higher traffic density, i.e.

0.01 a/c per Nm³. This resulted in choosing containers having a length of 40 Nm, a width of 40 Nm and a height of 3000 feet, and with 8 aircraft flying in such container.

By running the IPS algorithm ten times (+ one extra IPS run later on) over 20 minutes, with 5 minutes convergence time prior to this, the collision probability per unit time of flying has been estimated. The number of particles per IPS simulation run is 10,000. The total simulation time took about 300 hours on two machines, and the load of computer memory per machine was about 2.0 GigaByte. For the first four IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table IV for each of the conflict levels, $k = 1, \dots, 8$, for aircraft $i = 1$.

TABLE IV. FRACTIONS COUNTED DURING FOUR IPS RUNS OF SCENARIO 2

Level	1 st IPS	2 nd IPS	3 rd IPS	4 th IPS
1	0.922	0.917	0.929	0.926
2	0.567	0.551	0.560	0.559
3	0.665	0.666	0.674	0.676
4	0.319	0.331	0.323	0.321
5	0.370	0.367	0.371	0.379
6	0.181	0.158	0.162	0.171
7	0.130	0.209	0.174	0.145
8	0.067	0.005	0.094	0.066
Product of fractions	6.42×10^{-5}	6.76×10^{-6}	1.11×10^{-4}	6.99×10^{-5}

The estimated mean probability of collisions per 20 minutes aircraft flight equals 5.22×10^{-5} , which is equal to a probability of collisions per aircraft flight hour of 1.6×10^{-4} , with minimum and maximum values respectively a factor four lower and higher. We also verified that this risk value was not sensitive at all to the failure rates of the ASAS related technical systems.

One should be aware that this value has been estimated for the simulation model of the intended AMFF operation. Hence the question is what this means for the intended AMFF operation itself? By definition a simulation model of AMFF differs from the intended AMFF operation. If it can be shown that the combined effect of these differences on the risk level is small, then the results obtained for the simulation model may be considered as a good representation of the accident risk of the intended operation. In order to assess the combined effect of these differences there is need to perform a bias and uncertainty assessment [30], [31].

In order to better learn understanding what causes the collision risk of the simulation model to be relatively high, we performed an extra IPS run, and memorized in static memory for each particle the ancestor history at each of the eight levels. This allowed us to trace back what happened for the particles that hit the last level set (i.e. collision). There appeared to be five different collision events. Evaluation of these five collision events showed that all five happened under nominal safety critical conditions. Four of the five collisions were due to a growing number of multiple conflicts that could not be solved in time under the operational concept adopted. The fifth collision was of another type: at quite a late moment finally a

conflict between two aircraft was solved with a maneuver by one of the two aircraft. However because of this maneuver there was a sudden collision with a third nearby aircraft.

These detailed evaluations of the five collision events of the 11th IPS run also showed that a significant increase of collision risk is caused by the relatively small height (4000 ft) of a container. Because of this small height it happened that an aircraft in one container came in conflict with a copy of its own in a neighbouring container, and in such a situation there was an undesired limitation in conflict resolution options, and thus an undesired artificial increase in collision risk.

The results in this section seem to indicate that the key factor in the increased risk of collision for encounters with homogeneous traffic in the background - as opposed to the eight encountering aircraft scenario - are the multiple conflicts. Under the far higher traffic densities than what the AMFF operational concept was designed for, it is not always possible to timely solve a sufficiently high fraction of those multiple conflicts. On the basis of this finding one would expect that the collision risk would decrease faster than linear with a decrease in traffic density. The validity of this expectation is verified by the next scenario.

D. Reduction of aircraft density by a factor four

Now we enlarge the length and width of each container by a factor two. This means that the traffic density is gone down by a factor four. Hence the density is now $\frac{3}{4}$ of the density counted on 23rd July 1999 in the en-route area near Frankfurt. This still is a factor 2.5 higher than current average density above Europe. At the same time simulated flying time has been increased to 60 minutes (with 10 minutes prior flying to guarantee convergence).

By running four times the IPS algorithm the collision risk is estimated four times. The number of particles per IPS simulation run is 10,000. The total simulation time took about 280 hours on two machines, and the load of computer memory per machine was about 2.0 GigaByte. For these IPS runs, the estimated fractions $\bar{\gamma}_k^i$ are given in Table V for each of the conflict levels, $k = 1, \dots, 8$, for aircraft $i = 1$.

TABLE V. FRACTIONS COUNTED DURING FOUR IPS RUNS OF SCENARIO 3

Level	1 st IPS	2 nd IPS	3 rd IPS	4 th IPS
1	0.755	0.750	0.752	0.749
2	0.295	0.292	0.286	0.285
3	0.476	0.475	0.497	0.487
4	0.263	0.258	0.266	0.267
5	0.321	0.315	0.300	0.328
6	0.068	0.088	0.082	0.096
7	0.156	0.367	0.290	0.254
8	0.011	0.059	0.021	0.005
Product of fractions	1.07×10^{-6}	1.61×10^{-5}	4.31×10^{-6}	1.07×10^{-6}

The estimated mean probability of collision per aircraft flight hour equals 5.64×10^{-6} , with minimum and maximum values respectively a factor five lower and higher. This is about a factor 30 lower than the previous scenario with a four



times higher aircraft density. Thus, for the model there is a steep decrease of collision probability with decrease of traffic density, and this agrees well with the expectation at the end of the previous section.

E. Discussion of IPS simulation results

Because of the IPS simulation approach we were able to estimate collision risk for complex multiple aircraft scenarios. This is a major improvement over what was accomplished by [8] for a scenario of two free flight equipped aircraft that were supposed to fly within a fixed route structure. Inherent to the IPS way of simulation, the dynamic memory of the computers used appeared to pose the main limitation on the full exploitation of the novel sequential MC simulation approach. This also prevented performing a bias and uncertainty assessment for the differences between the simulation model and the AMFF operation. As long as such a bias and uncertainty assessment has not been performed, any conclusion drawn from the simulation apply to the simulation model only, and need not apply to the intended AMFF operation.

The simulations performed for a model of AMFF allow free flight operational concept developers to learn characteristics of the simulation model. Because of the sequential MC simulation based speed up, these simulations can show events that have not been observed before in MC simulations of an AMFF model. Under far higher traffic densities than what the AMFF operational concept has been designed for, the simulations of the model shows it is not always possible to timely solve multiple conflicts. As a result of this, at high traffic levels there is a significant chance that multiple conflicts are clogging together, and this eventually may cause a non-negligible chance of collision between aircraft in the simulation model. It has also been shown that by lowering traffic density, the chance of collision for the model rapidly goes down.

V. CONCLUDING REMARKS

This paper studied collision risk estimation of a free flight operation through a sequential Monte Carlo simulation. First a Monte Carlo simulation model of this free flight operational concept has been specified in a compositional way using the Stochastically and Dynamically Coloured Petri Net (SDCPN). Subsequently a novel sequential MC simulation method [32]-[34] has been extended for application to collision risk estimation in air traffic, and has subsequently been applied to an SDCPN model of free flight.

The results obtained clearly show that the novel simulation model specification and collision risk estimation methods allow to speed up Monte Carlo simulation for a much more complex simulation model than what was possible before (e.g. [8], [36]). Moreover, for the simulation model of the free flight operational concept considered, behavior has been made visible that was expected by free flight concept designers, but could not be observed in earlier Monte Carlo simulations: the rare

chance of clogging multiple conflicts at far higher traffic density levels than where the particular concept has been designed for. Hence, further attention has to be drawn towards the development and incorporation in the particular operational concept design of advanced methods in handling multiple conflicts. [4] studied a conflict resolution approach that performs better than the one adopted in the AMFF concept. In addition, there are some complementary developments that aim to develop complex conflict resolution solvers with guaranteed level of performance [37], [38], including ways to incorporate situation awareness views by human operators (pilots and/or controllers) in these combinatorial conflict resolution problems [39].

The main value of having performed this collision risk estimation for an initial simulation model of AMFF is that this provides valuable feedback to the design team and allows them to learn from Monte Carlo simulation results they have never seen before. This allows them to significantly improve their understanding when and why multiple conflicts are not solved in time anymore in the simulation model. Subsequently the operational concept designers can use their better understanding for adapting the AMFF design such that it can better bring into account future high traffic levels.

In its current form the sequential MC simulation approach works well, but at the same time poses very high requirements on the availability of dynamic computer memory and simulation time. The good message is that in literature on sequential MC simulation (e.g. [40]-[43]), complementary directions have been developed which remain to be explored for application to free flight collision risk estimation. These potential improvements of sequential MC simulation approach, and their application to free flight collision risk and bias and uncertainty estimation, will be studied in follow-up research.

REFERENCES

- [1] RTCA. Free Flight Implementation, Task Force 3 Final Technical Report, Washington DC, 1995.
- [2] NASA. Concept definition for distributed air-/ground traffic management (DAG-TM), Version 1.0, Advanced Air Transportation Technologies project, Aviation System Capacity Program, National Aeronautics and Space Administration, NASA, 1999.
- [3] J. Krozel. Free flight research issues and literature search. Under NASA contract NAS2-98005, 2000.
- [4] J. Hoekstra. Designing for Safety, the Free Flight Air Traffic Management concept, PhD Thesis, Delft University of Technology, November 2001.
- [5] FAA/Eurocontrol. Principles of Operations for the Use of ASAS, Cooperative R&D Action Plan 1 report, Version 7.1, 2001.
- [6] ICAO. Airborne separation assistance system (ASAS) circular, Draft, version 3, SCRSP, WGW/1 WP/5.0, International Civil Aviation Organization, May 2003.
- [7] FAA/Eurocontrol. Safety and ASAS applications, Co-operative R&D Action Plan 1 report, version 4.1, 2004.
- [8] M.H.C. Everdij, H.A.P. Blom, G.J. (Bert) Bakker. Modeling lateral spacing and separation for airborne separation assurance using Petri nets. *Journal of Simulation*, 2006.
- [9] B. Gayraud, F. Nacchia, J. Barff, R.C.J. Ruigrok, MFF operational concept, requirements and procedures, Report MFF D220, October 2005. www.medff.it/public/index.asp

- [10] J.W. Andrews, J.D. Welch, H. Erzberger. Safety analysis for advanced separation concepts. In *Proceedings of USA/Europe ATM R&D Seminar*, Baltimore, USA, 27–30 June 2005.
- [11] H. Erzberger. Transforming the NAS: The next generation air traffic control system. In *Proceedings of the 24th Int. Congress of the Aeronautical Sciences (ICAS)*, 2004.
- [12] MFF. MFF Final safety case, Report MFF D734, ed. 1.0. Available at <http://www.medff.it/public/index.asp>, November 2005.
- [13] R. Gordon, S.T. Shorrock, S. Pozzi, A. Boschiero, Predicting and simulating human errors in using the airborne separation assurance system procedure, *Human Factors and Aerospace Safety*, 2005.
- [14] R.C.J. Ruigrok, N. de Gelder, H.J. Abma, B. Klein Obbink, J.J. Scholte, Pilot perspective of ASAS self separation in challenging environments, Proc. 6th USA/Europe ATM R&D Seminar, Baltimore, USA, 27-30 June 2005.
- [15] D. Schaefer, C. Fusai, P. Scrivani, R. Waggin, Pilot evaluation of ASAS spacing applications under non-nominal conditions, Proc. 6th USA/Europe ATM R&D Seminar, Baltimore, USA, 27-30 June 2005.
- [16] A.P. Shah, A.R. Pritchett, K.M. Feigh, S.A. Kalarev, A. Jadhav, K.M. Corker, D.M. Holl, R.C. Bea. Analyzing air traffic management systems using agentbased modeling and simulation. In *Proceedings of the 6th USA/Europe Seminar on Air Traffic Management Research and Development*, Baltimore, USA, 27-30 June 2005.
- [17] K. Corker. Cognitive Models & Control: Human & System Dynamics in Advanced Airspace Operations, Eds: N. Sarter and R. Amalberti, *Cognitive Engineering in the Aviation Domain*, Lawrence Earlbaum Associates, New Jersey, 2000.
- [18] H.A.P. Blom, J. Daams and H.B. Nijhuis. Human cognition modeling in Air Traffic Management safety assessment. In *Air Transportation Systems Engineering*, edited by G.L. Donohue and A.G. Zellweger, Vol. 193 in Progress in Astronautics and Aeronautics, Paul Zarchan, Editor-in-Chief. Chapter 29, pages 481–511, 2001.
- [19] H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij, M.N.J. Van der Park. Human cognition performance model to evaluate safe spacing in air traffic. *Human Factors and Aerospace Safety*, Vol. 2, pages 59–82, 2003.
- [20] H.A.P. Blom, K.M. Corker, S.H. Stroeve. On the integration of human performance and collision risk simulation models of runway operation. In *Proceedings of the 6th USA/Europe Air Traffic Management R&D Seminar*, Baltimore, USA, 27–30 June 2005.
- [21] S.H. Stroeve, H.A.P. Blom and M.N. van der Park. Multi-Agent Situation Awareness Error Evolution in Accident Risk Modelling. In *Proceedings of the 5th USA/Europe Seminar on Air Traffic Management Research and Development*, Budapest, Hungary, 23-27 June 2003.
- [22] F. Maracich, Flying free flight: pilot perspective and system integration requirements, Proc. 24th DASC, Washington, 2005.
- [23] P.E. Labeau, C. Smidts and S. Swaminathan. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, Vol. 68, pages 219–254, 2000.
- [24] R. David, H. Alla. Petri Nets for the modeling of dynamic systems – A survey, *Automatica*, Vol. 30, No. 2, pages 175–202, 1994.
- [25] M.H.C. Everdij, H.A.P. Blom. Petri Nets and Hybrid state Markov Processes in a power-hierarchy of dependability models. In Proceedings of IFAC Conference on Analysis and Design of Hybrid Systems, Saint-Malo Brittany, France, pages 355–360, June 2003.
- [26] M.H.C. Everdij, H.A.P. Blom. Piecewise deterministic Markov processes represented by dynamically coloured Petri nets, *Stochastics*, Vol. 77, pages 1–29, 2005.
- [27] M.H.C. Everdij, H.A.P. Blom. Hybrid Petri nets with diffusion that have into mappings with generalised stochastic hybrid processes. In [40], pages 31–64, 2006.
- [28] G. Pola, M.L. Bujorianu, J. Lygeros, M.D. Di Benedetto. Stochastic hybrid models: an overview with applications to air traffic management. In *Proceedings of IFAC Conf. Analysis and Design of Hybrid Systems (ADHS)*, 2003.
- [29] M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom, B. Klein Obbink. Compositional specification of a multi-agent system by stochastically and dynamically coloured Petri nets. In [40], pages 325–350, 2006.
- [30] M.H.C. Everdij and H.A.P. Blom. Bias and uncertainty in accident risk assessment, NLR report CR-2002-137, National Aerospace Laboratory NLR, 2002.
- [31] M.H.C. Everdij, H.A.P. Blom, S.H. Stroeve. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. In Proceedings of the 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), New Orleans, USA, May 2006.
- [32] F. Cérou, P. Del Moral, F. Le Gland and P. Lezaud. Genetic genealogical models in rare event analysis, Publications du Laboratoire de Statistiques et Probabilités, Toulouse III, 2002.
- [33] F. Cérou, P. Del Moral, F. Le Gland, P. Lezaud. Limit theorems for the multilevel splitting algorithms in the simulation of rare events. In Proceedings of Winter Simulation Conference, Orlando, USA, 2005.
- [34] J. Krystul, H.A.P. Blom. Generalised stochastic hybrid processes as strong solutions of stochastic differential equations, Hybrid Report D2.3, 2005, see <http://www.nlr.nl/public/hosted-sites/hybrid/>
- [35] J. Krystul, H.A.P. Blom. Sequential Monte Carlo simulation of rare event probability in stochastic hybrid systems. In *Proceedings of the 16th IFAC World Congress*, Prague, Czech Republic, June 4-8, 2005.
- [36] H.A.P. Blom, G.J. Bakker, M.H.C. Everdij and M.N.J. van der Park. Collision risk modeling of air traffic. In *Proceedings of European Control Conference*, Cambridge, UK, 2003.
- [37] Lecchini, W. Glover, J. Lygeros, J. Maciejowski. Monte Carlo optimisation for conflict resolution in air traffic control. In [40], pages 257–276, 2006.
- [38] D.V. Dimarogonas, S.G. Loizou, K.J. Kyriapoulos. Multirobot navigation functions II: towards decentralization. In [40], pages 209–256, 2006.
- [39] E. De Santis, M.D. Di Benedetto, S. Di Gennaro, A.D. Innocenzo, G. Pola. Critical observability of a class of hybrid systems and application to air traffic management. In [40], pages 141–170, 2006.
- [40] H.A.P. Blom, J. Lygeros. *Stochastic Hybrid Systems: Theory and Safety Critical Applications*, LNCIS series, Springer, Berlin, 2006.
- [41] A. Doucet, N. de Freitas and N. Gordon. *Sequential Monte Carlo Methods in Practice*, Springer-Verlag, 2001
- [42] P. Glasserman. Monte Carlo Methods in Financial Engineering, Stochastic Modelling and Applied Probability, Vol. 53, Springer, 2003.
- [43] P. Del Moral. *Feynman-Kac Formulae. Genealogical and Interacting Particle Systems with Applications*, SpringerVerlag, New York, 2004.