HYBRIDGE

Distributed Control and Stochastic Analysis of Hybrid Systems
Supporting Safety Critical Real-Time Systems Design

WP9: Risk assessment for a distributed control system

Sequential Monte Carlo simulation of collision risk in free flight air traffic

**Authors: H. A.P. Blom, G.J. Bakker, J. Krystul, M.H.C. Everdij,
B. Klein Obbink and M.B. Klompstra**

31th August 2005

Version: *1.0*
Task number: *9.4*
Deliverable number: *PD22*
Contract: *IST-2001-32460 of European Commission*

DOCUMENT CONTROL SHEET

Title of document:	*Sequential Monte Carlo simulation of collision risk in free flight air traffic*
Authors of document:	*H.A.P. Blom, G.J. Bakker, J. Krystul, M.H.C. Everdij, B. Klein Obbink, M.B. Klompstra,*
Deliverable number:	*D9.4 = PD22*
Contract:	*IST-2001-32460 of European Commission*
Project:	*Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design (HYBRIDGE)*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
0.1	24th Feb. 2005	All	1st draft: creation of document
0.2	3rd March 2005	All	2nd draft
0.3	21st March '05	1,2,5	3rd draft
0.4	25th March '05	5,6	4th draft
0.5	31st March '05	6	5th draft
0.6	29th April 2005	All	Draft final for internal review
0.7	31th May 2005	All	Internal review comments incorporated
0.8	2nd June 2005	5,6	Some minor improvements
0.9	25th Aug 2005	All	Some further improvements
1.0	31st Aug 2005	6	Final version

Version 0.1		Organisation	Signature/Date
Authors	H.A.P. Blom	NLR	
	G.J. Bakker	NLR	
	J. Krystul	TWEN	
	M.H.C. Everdij	NLR	
	B. Klein Obbink	NLR	
	M.B. Klompstra	NLR	
Internal reviewers	R. Ruigrok	NLR	
	J. Hoekstra	NLR	

Abstract

Within HYBRIDGE a novel approach in speeding up Monte Carlo simulation of rare events has been developed. In the current report this method is extended for application to simulating collisions with a stochastic dynamical model of an air traffic operational concept. Subsequently this extended Monte Carlo simulation approach is applied to a simulation model of an advanced free flight operational concept; i.e. one in which aircraft are responsible for self separation with each other. The Monte Carlo simulation results obtained for this advanced concept show that the novel method works well, and that it allows studying rare events that stayed invisible in previous Monte Carlo simulations of advanced air traffic operational concepts.

CONTENTS

1. Introduction

1.1 Background of Hybridge project

The 21st century finds Europe facing a number of remarkable changes, many of which involve large complex real-time systems the management and control of which undergoes a natural trend of becoming more and more distributed while at the same time the safety criticality of these systems for human society tends to increase. Whatever good the control design for these systems will be, humans still carry responsibility for the operational safety. This implies that control system designs for safety critical operations have to be embedded within sound safety management systems such that the level of safety stays under control of humans. The objective of HYBRIDGE is to develop the methodologies to accomplish this, and to demonstrate their use in support of advanced air traffic management design.

In addition to direct application to air traffic management, these contributions form the nucleus for further research and development into a complex, uncertain system theory, and into application of this theory to distributed control of other real time complex systems such as communication, computer and power networks [Hybridge Project].

1.2 Main HYBRIDGE developments

Within the HYBRIDGE project distributed safety critical systems have been studied through three streams of research:

Stochastic hybrid modelling: Extension and unification of stochastic hybrid models. This topic has been addressed in the work packages (WPs) WP1, WP2 and WP4. WP1 studied the extension and unification of stochastic hybrid models from a stochastic automata perspective [D1.2], and has illustrated how these extensions are successfully used to the modelling of air traffic [D1.4]. WP2 studied the extension and unification of stochastic hybrid systems as semimartingale strong Markov solutions of stochastic differential equations on a hybrid state space [D2.3] and established an exact relation with executions of Petri nets [D2.4]. In addition, WP2 has illustrated the relevance of these extensions and relations for the modelling of accident risk in air traffic. WP4 has extended and generalized the compositional and analytical specification power of stochastic hybrid automata perspectivee, and has compared this with the Petri net formalism [D4.4].

Conflict resolution. This topic has been addressed along three complementary approaches; a potential field approach in WP3, stochastic optimization in WP5, and an analytical approach in WP6. The emphasis in WP3 was on the modelling and numerical evaluation of a probabilistic conflict prediction based potential field for air traffic. The numerical approaches considered are grid based evaluation [D3.1] and sequential Monte Carlo simulation [D3.2]. WP5 formulated the stochastic optimization problem within the very general and powerful paradigm of Model Predictive Control for a hybrid stochastic automaton [D5.2]. For an initial application to air traffic management a Markov Chain Monte Carlo method has shown to work well [D5.4]. WP6 has extended the Navigation functions approach developed in robotics conflict resolution for application to air traffic, and has demonstrated that the approach solves multiple conflicts in air traffic well for conflict situations that have a solution [D6.2].

Safety aspects have been studied in WP7, WP8 and WP9. The focus of WP7 was on the development of a systematic framework in observing and mitigating safety critical conditions in complex safety critical systems. An important objective of this framework development was an extension of the existing observability theory to handle the inherent non-observability of possibly deviating situation awareness by one or more human agents that are in charge to control the safety critical system [D7.5]. The focus of WP8 was on the development of novel ways to accelerate Monte Carlo simulations, and on the development of bias and uncertainty assessment for stochastic hybrid processes. First a review of the state of the art and the research on rare event Monte Carlo simulation in literature has been made [D8.2]. Stimulated by financial and communication industrial questions, strong developments appeared to be ongoing on multi-level and sequential Monte Carlo simulation methods [Doucet et al, 2001], [Glasserman 2003] and [Del Moral 2003]. The novel development that WP8 added to this was to study the combination of these two methods for stochastic hybrid processes that satisfy the strong Markov property. This has resulted into novel Interacting Particle System algorithms for rare event estimation [D8.3]. In addition to this the theory of bias and uncertainty assessment of [Everdij & Blom, 2002] has been extended to take into account the addition of risk stemming from different non-nominal modes of operation [D8.4]. Within WP9 the novel IPS approach has been applied to an advanced air traffic management example, the results of which are addressed by this report.

1.3 Objective and organisation of work package 9

The main objective of WP9 was to show the feasibility of applying and extending the modelling and rare event simulation methods developed within [D2.3], [D2.4], [D8.3] and [D8.4] towards:

- The development of a stochastic hybrid model of an advanced air traffic operation which includes appropriate models for the performance by the human agents that are in control of the safe and smooth air traffic behaviour.
- The assessment of collision risk for this stochastic hybrid model through using the novel multi-level and sequential Monte Carlo simulation approaches.

A complementary aim of WP9 was to derive from these results the relative value of the various results produced within the Hybridge work packages contribute to a safe advanced air traffic operation which makes explicit use of distributed control over multiple aircraft.

The WP9 work has been organised through the following four tasks:

Task 9.1: Identify an advanced air traffic operation, including a systematic identification of all non-nominal situations and hazards. The advanced air traffic operational concept selected is one of autonomous airborne separation assurance in en-route traffic. The result of this task has been reported in [D9.1]

Task 9.2: Develop a mathematically unambiguous stochastic hybrid model for the operation considered, and specify all model assumptions made, all model parameters and their values that are introduced. For this specification the approaches developed within WP2 are being applied, and are also extended to address additional problems. This task has been documented in [D9.2] and in [Bakker et al., 2005].

Task 9.3: Develop appropriate methods to assess collision risk of the Task 9.2 developed model through Monte Carlo simulation. For this, use is made of the rare event Monte Carlo simulation techniques developed in WP8, including their extension in order to handle the specifics of an advanced air traffic operation. This task has been documented in [D9.3]

Task 9.4: Perform the risk assessment with support of stochastic analysis and Monte Carlo simulations for the instantiated models and their software implementation, and assess the relative importance of the novel approaches developed within the various WPs for further development and application to advanced air traffic management. The results of this task and highlights of the results in [D9.1], [D9.2] and [D9.3] are documented in the current final report for WP9.

1.4 Organisation of this report

The report is organised as follows. Section 2 provides a brief overview of the Free Flight operational concept selected for evaluation on collision risk within WP9. Section 3 explains how this operational concept has been modelled in the novel Petri net formalism following a compositional specification approach. Next section 4 outlines the resulting Petri net for the free flight operation. Section 5 develops the Monte Carlo simulation acceleration algorithm to be applied to the free flight simulation model. Section 6 presents the results of the Monte Carlo simulations performed to estimate collision risk for the free flight simulation model. Section 7 draws conclusions for the novel way to speed up Monte Carlo simulation of collision risk in air traffic, and what this means for the other key complementary developments realized within the HYBRIDGE project.

2. Free flight air traffic

2.1 Current ATM

In the very early days of flying, a pilot initially navigated using ground features such as roads, rail tracks and coastlines. Soon beacons were placed creating a route structure in the sky consisting of so-called airways. By keeping a sharp look out, a pilot avoided collisions with other aircraft using some rules indicating who had right of way. Later on, radar and radio allowed air traffic controllers to separate traffic near airports in weather conditions previously inhibiting safe flight, and in airspace where pilots became uncomfortable with their look out task when traffic increased. Although modern navigation no longer relies on flying to and from a beacon, route structures still are in use as an instrument for air traffic control to work with organized traffic flows.

As a result of this development current Air Traffic Management (ATM) consists of:

- A set of rules in the sky: the Instrument Flight Rules (IFR);
- Air traffic controllers who, for their air space sector, are responsible for providing minimum separation (either 3/5Nm horizontally or 1000/2000 feet vertically);
- Ground surveillance by means of passive and active radar and information processing;
- Communication between pilots and air traffic controllers by radio telecommunication;
- A system for alerting an Air Traffic Controller of a conflict on the short term;
- Airborne systems, one per aircraft, for alerting and advising aircrew involved in collision avoidance in the rare case of a conflict not timely solved by air traffic control;
- Flow control management centres which take care that the en-route traffic load per sector stays below a level that can safely be handled by the air traffic controllers (15 – 20 aircraft);

Accommodation of more traffic by current ATM is realized by reducing the size of sectors. With decreasing sector size the rate of aircraft entering and leaving a sector is increasing. Beyond a certain point this jeopardizes the effectiveness of air traffic control, and this point seems to have been reached for multiple en route sectors over Europe and the USA. The free flight idea is that current technology should allow giving back conflict management responsibilities (partly) to pilots, and thus creating the possibility to increase traffic without decreasing sector size.

2.2 Advanced en route ATM: Free Flight

The development of advanced Airborne Separation Assurance System (ASAS) technology makes it possible for aircraft to broadcast information about the own-ship position and velocity to surrounding aircraft, and to receive similar information from surrounding aircraft. Because of this, it is possible to rethink the overall concept for today's Air Traffic Management. In particular, it might be possible in some airspace to transfer the complete responsibility for conflict prevention from ground to air. As the aircrews thus obtain the freedom to select their trajectory –that is: without the obligation to follow ATC instructions– the resulting concept is called Free Flight.

Free Flight –sometimes referred to as Self Separation Assurance– is a concept where pilots are allowed to select their trajectory freely at real time, at the cost of acquiring responsibility for conflict prevention ([ICAO ASAS Circ], [PO-ASAS], [Hoekstra, 2001]). 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, ATC sectorization and routes are removed and new technologies are brought in. It also plays an important role in the Distributed Air-Ground Traffic Management concept, which allows for distributed decision-making between flight deck, air traffic service providers and aeronautical operational control centres of airlines, for further optimisation of operations ([DAG-TM], [FFlit], [Erzberger, 2004]).

Free Flight is first characterised by the lack of a central control mechanism: conflicts between aircraft are not detected and solved by one dedicated agent. Instead, each individual aircrew has the responsibility to avoid conflicts, thereby assisted by navigation means, surveillance processing and equipment displaying conflict-solving trajectories. These system components and the pilots-flying and pilots-non-flying can be considered as agents that exchange information and collaborate (within and between aircraft). From this perspective, due to the potentially many aircraft involved and due to the relatively large number of agents involved in each aircraft, the system is highly distributed. This holds not only true for the functions and tasks, but also for the detection of conflicts, the traffic information exchange and the decision-making with respect to conflict solutions.

This abstract level of Free Flight concept definition leaves open many details of procedures, algorithms, equipment performance requirements, etcetera. Because of this, ATM concept designers have been and still are studying multiple Free Flight operational concepts and their implementation choices. One implementation choice is the level of co-ordination between aircraft (such as the need for confirmation of the conflict or for exchange of intended trajectories). Another aspect is whether the conflict resolution concept should be based on priority rules or on co-operative contributions. Such choices can be considered as control mechanisms in a distributed architecture. One of the Free Flight operational concept the implementation choices are quite well developed is an autonomous free flight concept for application to traffic flying between Europe and Africa. For short we refer to this operational concept as Autonomous Mediterranean Free Flight (AMFF).

2.3 AMFF enabling systems

There are several novel technical systems under development/deployment which enable AMFF. First of all, aircraft navigation is assumed to be based on Global Navigation Satellite System (GNSS), augmented and coupled with Inertial Navigation and Inertial Reference Systems (INS/IRS) and several independent airborne altimeters. Depending on the ground infrastructure, traditional systems as VOR, DME and NDB are sometimes also available.

Aircraft are supposed to be equipped with an ADS-B (Automatic Dependent Surveillance-Broadcast) system, i.e. a system that periodically broadcasts and continuously receives this information from other aircraft. The aircraft originating the broadcast does not need to know which systems are receiving the broadcast. Any air or ground based user may choose to receive and process this information. AMFF assumes that the following information elements are handled and provided by ADS-B:

- Aircraft identification
- Call Sign

- Address
- Category
- Aircraft state vector
- Horizontal position
- Vertical position
- Horizontal velocity
- Vertical velocity
- Emergency/priority status

Concerning the equipment required to transfers data over air to air paths, there are several technologies available, each with its own benefits and limitations. All aircraft are also equipped with classical Radio/Telecommunication (R/T) to ensure voice communications for (at least) non-routine and emergency use, for aircraft-aircraft and for aircraft-ATC communication.

The Airborne Separation Assurance System (ASAS) processes the information flows from the communication links, the navigation systems, the Flight Management System (FMS) and the auto-pilot. ASAS encompasses the conflict detection and resolution functionalities as described in the previous subsection. A control panel is the physical interface between the pilot, the display and the data processing, enabling the pilot to select the preferred features. ASAS related information is presented to the crew through a Cockpit Display of Traffic Information (CDTI). It can contain traffic information, selected waypoints, weather information, an airport map, proposed manoeuvres, virtual tunnels in the sky to guide the pilot, etceteras. The task of the CDTI is to inform the crew of the traffic around the aircraft, and aid them in the conflict handling. In particular, the CDTI shall enable the crew to monitor traffic e.g. by:

- Displaying position of local traffic: latitude/longitude or bearing/distance and altitude in same reference frame as the navigation information,
- Showing speeds of traffic: ground speed, track, and vertical speed,
- Indicating conflicts and possible manoeuvres to solve them,
- Leaving the crew the possibility de-clutter (deselect) the traffic information manually,

The CDTI also shows: conflict zones, dangerous areas, FFAS boundaries, segregated areas, transition zones, density of traffic in entry/exit points, forbidden headings, climb/descent sense and rates, speed ranges so as to avoid short-term conflicts. A CDTI typically is used in coordination with other systems, such as for example other Caution and Warning Systems, ACAS, Autoflight systems and FMS [ARP 5365]. If either ASAS or ACAS is tracking a target that is not tracked by the other system, the CDTI shows which of the two system has produced the target track.

2.4 Conflict detection and resolution within AMFF

The conflict detection and resolution approach developed for AMFF has its roots in the modified potential field approach [Hoekstra, 2001]. However the AMFF concept has some significant deviations from this in the form that conflict resolution algorithms are sometimes intentionally designed not to take the potential field of all aircraft into account. In order to indicate roughly the concept that is under study in this report, the following most important aspects are mentioned:

- 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 not broadcast and therefore assumed to be unknown.
- The vertical separation minimum is 1000 ft and the horizontal separation minimum is 5 Nm. The Airborne Separation Assistance System (ASAS) detects a conflict if the separation minima will be violated within 6 minutes.
- The conflict resolution process is split in a priority and a co-operative phase: in the first phase one aircraft gets priority while the crew of the other aircraft should make a resolution manoeuvre and in a second phase both crews should make a resolution manoeuvre.
- Conflict co-ordination does not take place explicitly, i.e. there is no communication on whether and how a resolution manoeuvre will be executed.
- The ASAS presents two conflict resolution manoeuvres: one in the vertical and one in the horizontal plane. It is the pilot who decides which manoeuvre to execute.

In the ATM community, the discussion about the level of automation, embedded computation and the precise roles of the pilots in the choice of a conflict resolution manoeuvre (especially in case of inconsistent traffic information) is ever present. For AMFF the tendency so far is to make the concept quite lean and mean, in order to avoid much information exchange between systems and to avoid dedicated, smart but potentially incomprehensible decision-making by artificial intelligent machines. The aircrew carries full responsibility for operational safety and is therefore in control of each safety critical sub-procedure. In particular, the airborne equipment gives advices on potential manoeuvres, but it is the pilot who decides and actually executes. As result of this, the AMFF proposed conflict resolution algorithms are to some extend 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 [Hoekstra, 2001].

Although results of initial studies show that en route application of Free Flight seems feasible, it is not clear yet what this means relative to ICAO's Target Level of Safety. In particular it is not clear which traffic loads can safely be accommodated under the AMFF operational concept. In order to improve this, the next step is to develop and run a Monte Carlo collision risk simulation model of this AMFF operation.

3. Compositional specification of a Petri Net model

3.1 Compositional specification challenge

By the very nature of ATM in general, and of free flight in particular, the various human decision-makers are highly distributed (e.g. at least there is a crew of pilots per aircraft). In addition, the safety related decision-making process involves interactions of humans with each other and with:

- a random and often unpredictable environment, e.g. varying wind, thunderstorms, etc.,
- a large set of procedural rules and guidelines,
- many technical and automation support systems,
- decision-makers at airline operation centres.

These aspects make accident risk assessment for free flight operations a very challenging application area, the decision making process of which is significantly more complex than it is of operations in other safety-critical industries as is illustrated in Figure 1. This makes the specification of an unambiguous mathematical model of free flight operations a very challenging task.

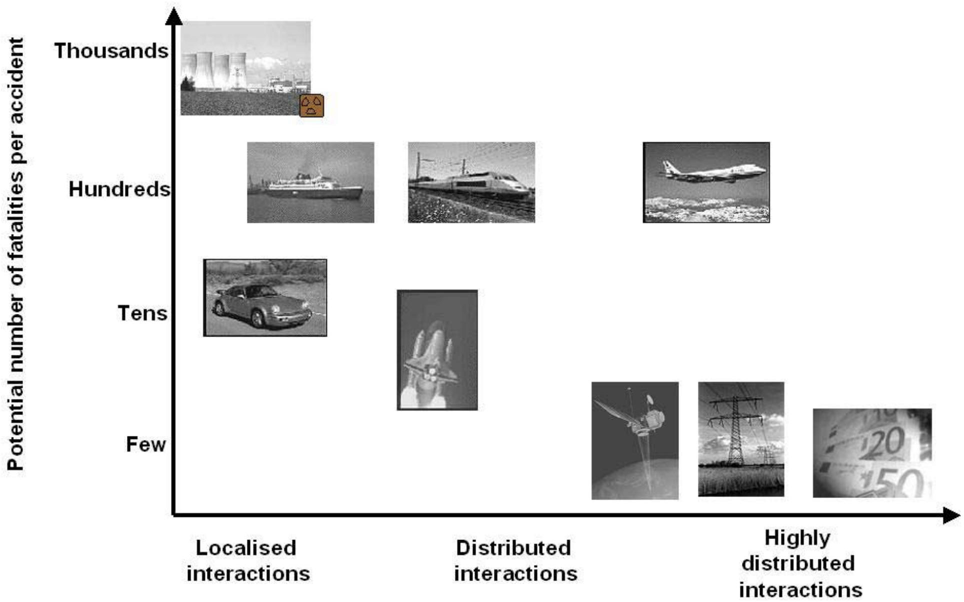

Fig. 1. Potential fatalities and distribution level of air traffic and other safety-critical operations.

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. Labeau et al, 2000) 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. David & Alla, 1994). 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, Everdij & Blom (2003a, 2005) introduced Dynamically Coloured Petri Net (DCPN) and Stochastically and Dynamically Coloured Petri Net (SDCPN), and proved that there exists a close relationship with the larger class of stochastic processes and analysis techniques needed for air traffic operations (Everdij & Blom, 2003b). Basically, an SDCPN is an extension of Coloured Stochastic Petri Net (e.g. Haas, 2002), in the sense that in SDCPN the token colours evolve in time (dynamically) as solutions of differential equations while the tokens reside in their places. Since its introduction, the SDCPN formalism has been successfully used in practical air traffic applications, (e.g. Blom et al, 2003b, 2003c). However, it was found that when being used for modelling more and more complex multi-agent hybrid systems, the compositional specification power of Petri nets reaches its limitations. More specifically, the following problems were identified:

A. **Need for a hierarchy from low level Petri nets to the complete Petri net.** For the modelling of a complete Petri net for complex systems, a hierarchical approach is necessary in order to be able to separate local modelling issues from global or interaction modelling issues.
B. **Duplication of arcs and transitions within a low level Petri net.** Often the addition of an interconnection between two low-level Petri nets leads to a duplication of transitions and arcs in the receiving Petri net.
C. **Cluttering of interconnections.** The number of interconnections between the different low level Petri nets tends to grow quadratically with the size of the Petri net.

3.2 State of the art

In literature, several approaches have been developed to address problem A. Huber et al, (1990) introduced Hierarchical Coloured Petri Nets. These Hierarchical CPNs allow a set of subnets, called pages, to be related to each other, in such a way that together they constitute a single model. The pages interact with each other in a well-defined way. A page can also be substituted by a place or a transition, in order to show its role in the larger model, or to postpone its detailed modelling until later. In addition to these substitution transitions and places, Hierarchical CPN allow invocation transitions (CPN is temporarily extended with a new instance of an invocation subpage), place fusion (a set of places is folded into a single place) and transition fusion (a set of transitions is folded into a single transition). The pages that interact solve problem A.

More recent approaches also address problem A; they consider elementary Petri nets that have input (or entry) and output (or exit) places through which these Petri nets are coupled with other Petri nets. One example approach is $B(PN)^2$ (Basic Petri Net Programming Notation), introduced by Best and Hopkins (see e.g. Fleischhack & Grahlmann, 1997). The compositional denotational semantics of $B(PN)^2$ programs can be given in terms of M-nets (modular multilabelled nets), which form an algebra of composable high-level Petri nets. These Petri net components have at least one entry place and at least one exit place. Several composition operations (e.g. parallel composition, sequential composition) are defined to couple the Petri nets. Communication is performed by transition synchronisation. Another example approach is by Kindler (1997), who introduced the concept of Petri net Components and showed how systems can be composed from components. These components have input and output places and components can be connected at these input and output places. Kindler also provides the compositional semantics.

Also addressing problem A are Fernandes et al (1997) and Fota et al (1997), who consider sub-Petri nets that model parallel systems, and draw these sub-Petri nets in separate boxes. Places and transitions in different sub-Petri nets are coupled by arcs to model interactions. Fernandes et al (1997) uses Synchronous Interpreted Petri Nets (SIPN) as basis and shows how the interactions can be used to model synchronisation or priority of the parallel systems. Fernandes also allows hierarchy: a macroplace can be exploded (or imploded) to form (or hide) a complete sub-Petri net. Fota et al (1997) uses Generalized Stochastic Petri nets (GSPNs), refers to the sub-Petri nets as modules, and adopts the requirement that there should be exactly one token in each module; transitions in a module are not allowed to consume a token from another module without returning one immediately. Therefore, Fota introduced three module coupling mechanisms: 1) marking tests; 2) common transitions; 3) interconnection blocks. In addition, in order to improve the compactness of the module, Fota recommends two rules, called optimisation rules: 1) avoidance of immediate internal transitions; 2) module folding using memories.

For addressing problem B, some ideas from literature are useful. In order to avoid the duplication of transitions, one might apply transition fusion as proposed by Huber et al (1990), or module folding of Fota et al (1997).

3.3 Petri Net Model specification approach used

Within WP9, PN model specification approaches from literature are adopted to solve problem A, and novel approaches are developed to solve problems B and C. Together, these approaches are integrated into a compositional specification approach for SDCPN, which is explained below.

To solve problem A, the compositional specification of an SDCPN for a complex process or operation starts with developing a Local Petri Net (LPN) for each agent that exists in the process or operation (e.g. air traffic controller, pilot, navigation and surveillance equipment). Counterparts of LPNs in literature are the modules of Fota et al (1997), the pages of Huber et al (1990) and the components of Kindler (1997). An essential difference is that our LPNs (and Fota’s modules) are connected with each other in such a way that the number of tokens residing in an LPN is not influenced by these interconnections, while Huber and Kindler do not pose this restriction. Each LPN is surrounded by a box as done by e.g. Kindler (1997) and Fernandes et al (1997).

We use two types of interconnections 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, including Fota et al (1997) for inhibitor arcs and Fernandes et al (1997) for both types.
- Interaction Petri Net (IPN) from one (or more) transition(s) in one LPN to one (or more) transition(s) in another LPN. These IPNs are similar to the interconnection blocks of Fota et al (1997). If an IPN consists of one place only, then the connection of two LPNs through an IPN also has some similarity with place fusion, see e.g. Huber et al (1990) or Kindler (1997), except that our IPN will not change the number of tokens in its connecting LPNs.

Next, to solve problems B and C, we identify additional interconnections between LPNs that allow, with well-defined meanings, arcs to initiate and/or to end on the edge of the box surrounding an LPN. To the authors' knowledge this element has no counterpart in Petri net literature; however, it is based on how Harel (1987) composes statecharts. The meaning of these interconnections from or to an edge of a box allows several arcs or transitions to be represented by only one arc or transition. In that sense, there is a relation with transition fusion used by Huber et al (1990) and with module folding used by Fota et al (1997).

4. Petri Net model of Free Flight air traffic

The compositional specification approach of Section 3 is now used to specify an initial SDCPN model (Bakker et al., 2005) for a risk assessment of the Free Flight based air traffic operation adopted. The aim of this section is to illustrate the resulting SDCPN model. Next, in Section 5, it is explained how this model is used to perform Monte Carlo simulations.

4.1 LPNs of the Free Flight air traffic example

In the Free Flight air traffic example, the airspace is an En-Route Airspace without fixed routes or an active ATC specifying routes. All aircraft flying in this airspace are assumed to be properly equipped and enabled for Free Flight: the pilots can try to optimise their trajectory, due to the enlarged freedom to choose path and flight level. The pilots are only limited by their responsibility to maintain airborne separation, in which they are assisted by ASAS. This can be considered as a system processing the information flows from the data-communication links between aircraft, the navigation systems and the aircraft guidance and control systems. ASAS detects conflicts, alerts the crew, determines conflict resolution manoeuvres and presents the relevant information.

The number of agents involved in the Free Flight operation is huge and ranges from the Control Flow Management Unit to flight attendants. In the setting chosen for an initial risk assessment, the following agents are taken into account:

- A Pilot-Flying in each aircraft,
- A Pilot-Non-Flying in each aircraft,
- A number of systems and entities per aircraft, like the aircraft's position evolution and the Conflict Management Support systems,
- A number of global systems and entities, like the communication frequencies and the satellite system.

LPNs are specified for each relevant entity of each agent. It was judged sufficient to specify the following number of LPNs for the agents:

- 6 LPNs for each Pilot-Flying,
- 2 LPNs for each Pilot-Non-Flying,
- 36 LPNs for the systems and entities of each aircraft,
- 7 LPNs for the environment.

The actual number of LPNs in the whole model then depends on the number N of aircraft involved, and equals $7 + N \times (6 + 2 + 36)$.

4.2 Interconnected LPNs of "Pilot Flying"

This subsection illustrates, for the specific Free Flight air traffic example, a Petri Net model for the Pilot Flying as agent. 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 a LPN that does not belong to the Pilot-Flying as agent and is therefore 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 Fig. 2.

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.

There are many interactions (which, in some cases, are complex) between these individual LPNs, which are depicted as enabling arcs and IPNs with one place only. The use of the new interconnection mapping types makes that the figure is still readable. Table 1 shows that without the use of these interconnection mapping types the figure really would be cluttered with duplicated transitions and arcs within LPNs, and with connections drawn between LPNs.

Table 1. Numbers of interconnection mapping types and Petri net elements before and after application of interconnection mapping types. The number of places (i.e. 19 places within LPNs and 8 places between LPNs) does not change due to the interconnection mapping types.

Number of elements	In Figure 2		Without interconnection mapping types	
Within LPNs	27	transitions	279	transitions
	66	arcs	642	arcs
Between LPNs	16	ordinary arcs	293	ordinary arcs
	7	enabling arcs	1023	enabling arcs
	1	inhibitor arc	7	inhibitor arcs
Total	117		2244	

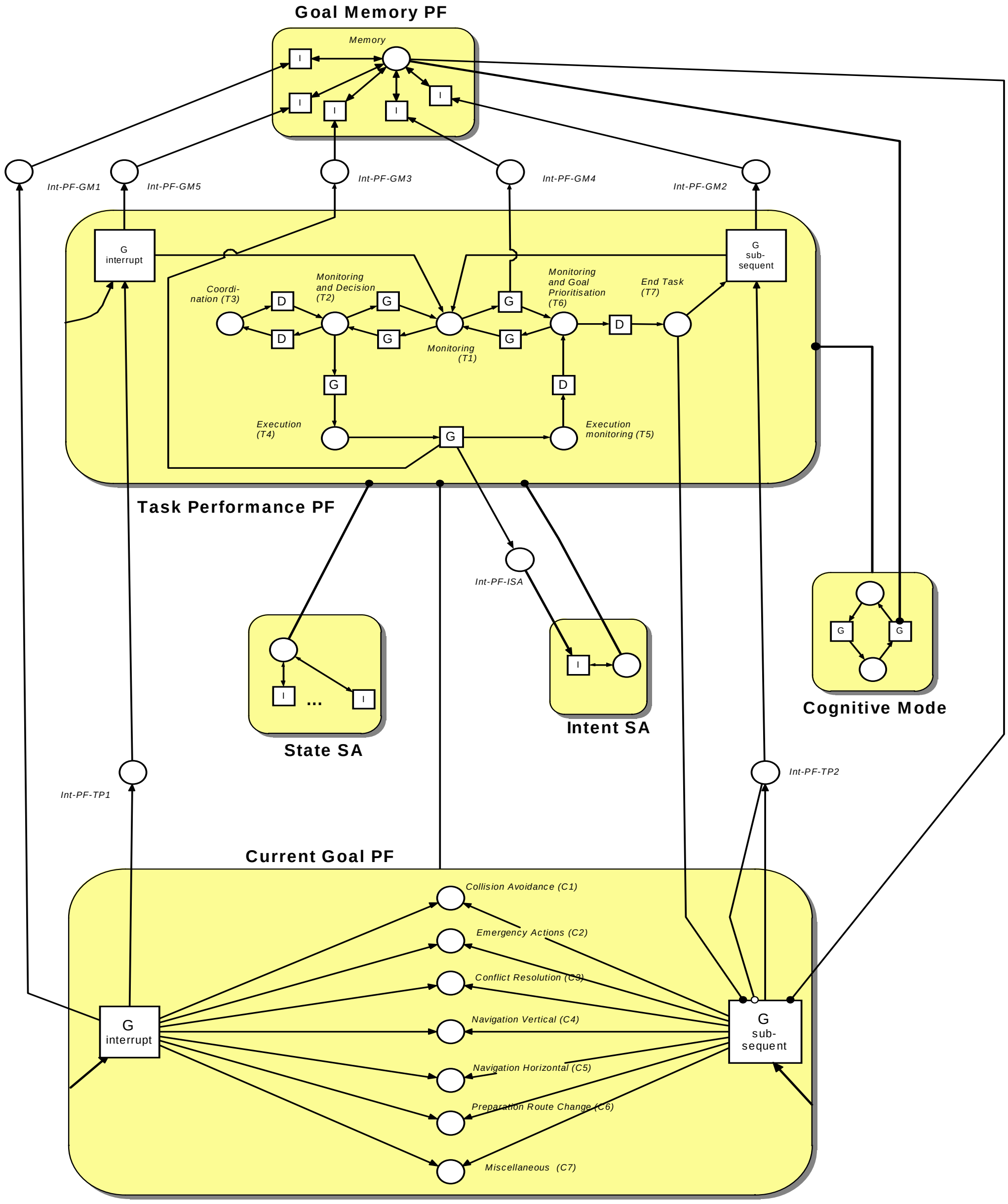

Fig. 2. The agent Pilot-Flying in Free Flight is modelled by 6 different LPNs, and a number of ordinary and enabling arcs and some IPNs, consisting of one place and input and output arcs.

5. Monte Carlo simulation of collision risk

The next step is to determine the collision risk of the free flight operation. The idea is to perform many Monte Carlo simulations with the SDCPN model specified for the free flight operation and, while doing so, to estimate the collision risk by counting the number of collisions and divide this by the number of simulated flight hours. Though this idea is simple, 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 Interacting Particle System (IPS) approach of Cérou et al. (2002) to collision risk assessment in air traffic.

5.1 Simulation to first moment of collision

Throughout this and the next sections, all stochastic processes are defined on a complete stochastic basis (Ω, F, $\mathbb{F}$, P, $\mathbb{T}$) with (Ω, F, P) a complete probability space, and $\mathbb{F}$ is an increasing sequence of sub-σ-algebra's on the positive time line $\mathbb{T}=\mathbb{R}_+$, i.e. $\mathbb{F} \triangleq \{J,(F_t, t\in \mathbb{T}), F\}$, J containing all P-null sets of F and $J \subset F_s \subset F_t \subset F$ for every $s < t$.

In [D2.4] it has been shown that an SDCPN model can be represented as the solution of a stochastic differential equation (SDE) on a hybrid state space, driven by Brownian motion and Poisson random measure. In [D2.3] it has been shown that under reasonable conditions (typically also adopted when specifying an SDCPN) the solution of this SDE is a strongly unique hybrid state process $\{x_t, \theta_t\}$ which is both a semimartingale and a strong Markov process. For an N-aircraft free flight traffic scenario the process $\{x_t, \theta_t\}$ consists of components $x_t \triangleq \mathrm{Col}\{x_t^0, x_t^1, \ldots, x_t^N\}$ and $\theta_t \triangleq \mathrm{Col}\{\theta_t^0, \theta_t^1, \ldots, \theta_t^N\}$, x_t^i assumes values from $\mathbb{R}^{n_i}$, and θ_t^i assumes values from a finite set (M^i). Physically, $\{x_t^i, \theta_t^i\}$, $i = 1,\ldots,N$, 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 process $\{x_t, \theta_t\}$ is $\mathbb{R}^n \times M$ -valued with $n = \sum_{i=0}^{N} n_i$ and $M = \prod_{i=0}^{N} M_i$.

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 two aircraft (i, j). The relative horizontal position is obtained through the mapping $y^{ij}(x_t)$, the relative horizontal velocity is obtained through the mapping $v^{ij}(x_t)$. The relative vertical position is obtained through the mapping $z^{ij}(x_t)$, and vertical rate of climb/descent is obtained through the mapping $r^{ij}(x_t)$. The relation between these position and velocity mappings satisfies the following two equations:

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

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

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:

$$D^{ij} = \{x \in \mathbb{R}^n;\ \left|y^{ij}(x)\right| \le (l_i + l_j)/2 \text{ AND } \left|z^{ij}(x)\right| \le (s_i + s_j)/2\}, \qquad i \ne j \tag{3}$$

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:

$$D^{ij} = \{x \in \mathbb{R}^n;\ \left|y^{ij}(x)\right| \le l \text{ AND } \left|z^{ij}(x)\right| \le s\}, \qquad i \ne j \tag{4}$$

Although all aircraft have the same size, notice that in (4), D^{ij} still 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.

$$\tau^{ij} = \inf\{t > 0;\ x_t \in D^{ij}\}, \qquad i \ne j \tag{5}$$

The first moment τ^i of collision with any of the other aircraft, i.e.

$$\tau^i = \inf_{j \ne i}\{\tau^{ij}\} = \inf_{j \ne i}\{t > 0;\ x_t \in D^{ij}\} = \inf\{t > 0;\ x_t \in D^i\} \tag{6}$$

with $D^i = \bigcup_{j \ne i} D^{ij}$

From this moment τ^i on, we assume that the differential equations for $\{x_t^i, \theta_t^i\}$ stop evolving. An unbiased estimation procedure of the risk 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 $\tau^i < T$.

5.2 Risk factorization using multiple conflict levels

Cérou et al. (2002) have developed a novel way of speeding up Monte Carlo simulation to estimate the probability that an $\mathbb{R}^n$-valued strong Markov process x_t hits a given "small" subset $D \in \mathbb{R}^n$ within a given time period (0,T). This method essentially consists of taking advantage of an appropriately nested sequence of closed subsets of $\mathbb{R}^n$: $D = D_m \subset D_{m-1} \subset \ldots \subset D_1$, and then start simulation from outside D_1, and subsequently simulate from D_1 to D_2, from D_2 to D_3, …, and finally from D_{m-1} to D_m. In order to apply this approach to the free flight operational concept considered we identified the following approach in defining a sequence of nested subsets.

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

$$D_k^{ij} = \{x \in \mathbb{R}^n;\ \left|y^{ij}(x) + \Delta v^{ij}(x)\right| \le d_k \text{ AND } \left|z^{ij}(x) + \Delta r^{ij}(x)\right| \le h_k, \text{ for some } \Delta \in [0, \mathrm{T}_k]\},\ i \ne j \quad (7)$$

with d_k, h_k and T_k the parameters of the conflict definition at level *k*, and with $d_m = l$, $h_m = s$ and $T_m = 0$, and with $d_{k+1} \ge d_k$, $h_{k+1} \ge h_k$ and $T_{k+1} \ge T_k$. 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 last 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.

$$\tau_k^i = \inf_{j \ne i}\{\tau_k^{ij}\} = \inf_{j \ne i}\{t > 0;\ x_t \in D_k^{ij}\} = \inf\{t > 0;\ x_t \in D_k^i\} \quad (9)$$

with $D_k^i \stackrel{\Delta}{=} \bigcup_{j \ne i} D_k^{ij}$

Following the approach of Cérou et al. (2002), next we define {0,1}-valued random variables $\{\chi_k^i, k = 1,..,m\}$ as follows:

$$\begin{aligned} \chi_k^i &= 1, \text{ if } \tau_k^i < T \text{ or } k = 0 \\ &= 0, \text{ else} \end{aligned}$$

By using this χ_k^i definition 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:

$$\mathbb{P}(\tau_m^i < T) = \mathbb{E}[\chi_m^i] = \mathbb{E}[\prod_{k=1}^m \chi_k^i] = \prod_{k=1}^m \mathbb{E}[\chi_k^i \left| \chi_{k-1}^i = 1\right.] = \prod_{k=1}^m \mathbb{P}(\tau_k^i < T \left| \tau_{k-1}^i < T\right.) = \prod_{k=1}^m \gamma_k^i \quad (10)$$

with $\gamma_k^i \stackrel{\Delta}{=} \mathbb{P}(\tau_k^i < T \left| \tau_{k-1}^i < T\right.)$

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. Because of the multiplication of the various individual γ_k^i estimators, which depend on each other, in general such a product may be heavily biased. The key novelty of Cérou et al. (2002) 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. This approach is explained next.

5.3 Characterization of the risk factors under strong Markov property

Let us denote $E' = \mathbb{R}^{n+1} \times M$, and let $\mathcal{E}'$ be the Borel $\sigma-$algebra of E'. For any $B \in \mathcal{E}'$, $\pi_k^i(B)$ denotes the conditional probability of $\xi_k \stackrel{\Delta}{=} (\tau_k, x_{\tau_k}, \theta_{\tau_k}) \in B$ given $\chi_l^i = 1$ for $1 \le l \le k$.

Define $\bar{D}_k^i = (0,T) \times D_k^i \times M$, $k = 1,\ldots,m$. Then the estimation of the probability for ξ_k to arrive at the k-th nested Borel set $\bar{D}_k^i$ is characterized through the following recursive sequence of transformations

$$\begin{array}{ccc} \pi_{k-1}^i(\cdot) \xrightarrow{\text{prediction}} & p_k^i(\cdot) & \xrightarrow{\text{conditioning}} \pi_k^i(\cdot), \\ & \downarrow & \\ & \gamma_k^i & \end{array}$$

where $p_k^i(B)$ is the conditional probability of $\xi_k \in B$ given $\chi_l^i = 1$ for $0 \le l \le k-1$. Because $\{x_t, \theta_t\}$ is a strong Markov process, $\{\xi_k\}$ is a Markov sequence, the prediction of which satisfies:

$$p_k^i(B) = \int_{E'} p_{\xi_k|\xi_{k-1}}(B \mid \xi)\pi_{k-1}^i(d\xi) \text{ for all } B \in \mathcal{E}', \tag{11}$$

Next we characterize the conditional probability of reaching the next level:

$$\begin{aligned} \gamma_k^i &= \mathbb{P}(\tau_k^i < T \mid \tau_{k-1}^i < T) \\ &= \mathbb{E}[\chi_k^i \mid \chi_{k-1}^i = 1] \\ &= \int_{E'} 1_{\{\xi \in \bar{D}_k^i\}} p_k^i(d\xi). \end{aligned} \tag{12}$$

And the conditioning satisfies:

$$\pi_k^i(B) = \frac{\int_B 1_{\{\xi \in \bar{D}_k^i\}} p_k^i(d\xi)}{\int_{E'} 1_{\{\xi' \in \bar{D}_k^i\}} p_k^i(d\xi')} \text{ for all } B \in \mathcal{E}'. \tag{13}$$

With this, each of the m terms γ_k^i in (10) is characterized as a solution of a sequence of “filtering” kind of equations (11)-(13). An important difference with “filtering” equations is however that (11)-(13) are ordinary integral equations, i.e. they have no stochastic term entering them.

5.4 Interacting Particle System based risk estimation

For simulation from D_{k-1}^i to D_k^i a fraction $\bar{\gamma}_k^i$ of the Monte Carlo simulated trajectories will reach D_k^i within the time period (0,T). Cérou et al (2002) have proven, under certain conditions how to manage the simulations from D_{k-1}^i to D_k^i, that the product of these fractions $\bar{\gamma}_k^i$ forms an unbiased estimate of the probability of x_t to hit the set D^i within the time period (0,T) , i.e.

$$\mathbb{E}[\prod_{k=1}^m \bar{\gamma}_k^i] = \prod_{k=1}^m \gamma_k^i = \quad \mathbb{P}(\tau^i < T)$$

and also that there is some bound on the expected estimation error. A version of this Interacting Particle System (IPS) simulation algorithm is explained next.

In [Krystul&Blom, 2005] the method of Cerou et al. (2002) has been extended to the situation of a strong Markov process in a hybrid state space. Here we apply this to the multi aircraft SDCPN model of subsection 5.1. The transformations (11)-(13) lead to the IPS algorithm of (Cérou et al., 2002) to estimate $\mathbb{P}(\tau_m^i < T)$. Following Krystul & Blom (2004), this algorithm can be specified as follows, where $\bar{\gamma}_k^i$, $\bar{p}_k^i$ and $\bar{\pi}_k^i$ denote the numerical approximations of γ_k^i, p_k^i and π_k^i respectively:

Step 0. Initial sampling; $k = 0$.

- For $l = 1,\ldots,N_p$ generate initial state value outside $\bar{D}_1^i$ by independent drawings (x_0^l, θ_0^l) from $p_{x_0,\theta_0}(\cdot)$ and set $\xi_0^l = (0, x_0^l, \theta_0^l)$
- For $l = 1,\ldots,N_p$ set the initial weights: $\omega_0^l = 1/N_p$.
- Then $\bar{\pi}_0^i = \sum_{l=1}^{N_p} \omega_0^l \delta_{\{\xi_0^l\}}$.

Iteration k; $k = 1,\ldots,m$ over step 1 (prediction), step 2 (assess fraction), step 3 (conditioning) and step 4 (resampling).

Step 1. Prediction: $\pi_{k-1}^i \longrightarrow p_k^i$, based on eq. (11);

- For $l = 1,\ldots,N_p$ simulate a new path of the hybrid state Markov process, starting at ξ_{k-1}^l until the k-th set $\bar{D}_k^i$ is hit or $t=T$ (the first component of ξ_k^l counts time).
- This yields new particles $\{\hat{\xi}_k^l, \omega_{k-1}^l\}_{l=1}^{N_p}$.
- $\bar{p}_k^i$ is the empirical distribution associated with the new cloud of particles: $\bar{p}_k^i = \sum_{l=1}^{N_p} \omega_{k-1}^l \delta_{\{\hat{\xi}_k^l\}}$.

Step 2. Assess fraction: γ_k^i , based on eq. (12);

- The particles that do not reach the set $\bar{D}_k^i$ are killed, i.e. we set $\hat{\omega}_k^l = 0$ if $\hat{\xi}_k^l \notin \bar{D}_k^i$ and $\hat{\omega}_k^l = \omega_{k-1}^l$ if $\hat{\xi}_k^l \in \bar{D}_k^i$.
- Approximation: $\gamma_k^i \approx \bar{\gamma}_k^i = \sum_{l=1}^{N_p} \hat{\omega}_k^l$. If all particles are killed, i.e. $\bar{\gamma}_k^i = 0$ then the algorithm stops without $\mathbb{P}(\tau^i < T)$ estimate.

Step 3. Conditioning: $p_k^i \longrightarrow \pi_k^i$, based on eq. (13);

- The non-killed particles form a set S_k^i , i.e. iff $\hat{\xi}_k^l \in \bar{D}_k^i$, then particle $\{\hat{\xi}_k^l, \hat{\omega}_k^l\}$ is stored in S_k^i.

- Renumbering the particles in S_k^i yields a set of particles $\{\tilde{\xi}_k^l, \tilde{\omega}_k^l\}_{l=1}^{N_{S_k}}$ with N_{S_k} the number of particles in S_k^i.

Step 4. Resampling of π_k^i

- Resample N_p particles from S_k^i according to the following scheme:
  - if $\frac{1}{2} N_p \le N_{S_k} \le N_p$ then
    1. Copy the N_{S_k} particles, i.e. $\xi_k^l = \tilde{\xi}_k^l$ and set $\omega_k^l = \tilde{\omega}_k^l . \dfrac{N_{S_k}}{\bar{\gamma}_k^i . N_p}$ for $l = 1, \ldots, N_{S_k}$; the total weight of these particles is $\dfrac{N_{S_k}}{N_p}$,
    2. Draw $N_p - N_{S_k}$ particles ξ_k^l independently from the empirical measure $\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \delta_{\{\tilde{\xi}_k^l\}}$ and set $\omega_k^l = \dfrac{\sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l}{\bar{\gamma}_k^i . N_p} = \dfrac{1}{N_p}$; the total weight of these particles is $1 - \dfrac{N_{S_k}}{N_p}$.
  - if $N_{S_k} < \frac{1}{2} N_p$ then
    1. Copy the N_{S_k} particles, i.e. $\xi_k^l = \tilde{\xi}_k^l$ and set $\omega_k^l = \tilde{\omega}_k^l . \dfrac{1}{2.\bar{\gamma}_k^i}$ for $l = 1, \ldots, N_{S_k}$; the total weight of these particles is $\dfrac{1}{2}$,
    2. Draw $N_p - N_{S_k}$ particles ξ_k^l independently from the empirical measure $\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \delta_{\{\tilde{\xi}_k^l\}}$ and set $\omega_k^l = \dfrac{\sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l}{2.\bar{\gamma}_k^i.(N_p - N_{S_k})} = \dfrac{1}{2.(N_p - N_{S_k})}$; the total weight of these particles is $\dfrac{1}{2}$.

- The new set of particles is $\{\xi_k^l, \omega_k^l\}_{l=1}^{N_p}$.
- If $k < m$ then repeat steps 1, 2, 3, 4 for $k := k+1$.
- Otherwise, stop with $\mathbb{P}(\tau^i < T) \approx \prod_{k=1}^{m} \bar{\gamma}_k^i$.

Remark: In [D8.3] and [D9.3] the following resampling step 4 has been proposed:
Draw N_p particles ξ_k^l independently from the empirical measure

$\bar{\pi}_k^i = \sum_{l=1}^{N_{S_k}} \tilde{\omega}_k^l \delta_{\{\tilde{\xi}_k^l\}}$ each of which gets weight $\omega_k^l = \dfrac{1}{N_p}$

For this resampling step (Cérou et al., 2002) proved that the resulting estimate is unbiased, i.e.

$$\mathbb{E}[\prod_{k=1}^{m} \overline{\gamma}_k^i] = \mathbb{P}(\tau^i < T)$$

and also that:

$$(\mathbb{E}(\prod_{k=1}^{m} \overline{\gamma}_k^i - \prod_{k=1}^{m} \gamma_k^i)^p)^{\frac{1}{p}} \leq \frac{a_p b_p}{\sqrt{N_p}},$$

for some finite constants a_p and b_p, which depend on the simulated scenario, the multiple levels adopted and the number of particles used.

6. Simulation scenarios and collision risk estimates

The IPS method of section 5 is now applied to four aircraft scenarios. The first scenario has two aircraft, the flight plans of which cause the aircraft to be on a head on collision course. The second scenario has eight aircraft that fly at the same flight level and their flight plans cause them to fly through the same point in space at the same moment in time. The third 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 fourth scenario is the same as the third, except with a container that is twice as large in width and length.

6.1 Parameterization of the IPS simulations

The main safety critical parameter settings of the free flight enabling technical systems (GNSS, ADS-B and ASAS) are given in the following table.

Model Parameter	Probability
Global GNSS down	1.0×10^{-5}
Global ADS-B down*	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 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. These values are given in the first table.

k	1	2	3	4	5	6	7
d_k	5 Nm	5 Nm	5 Nm	2.5 Nm	1.25Nm	0.5 Nm	a/c length
h_k	1000 ft	1000 ft	1000 ft	1000 ft	500 ft	250 ft	a/c height
T_k	8 min	3 min	0 min	0 min	0 min	0 min	0 min

Next, during some 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 the next table. The main change was a splitting of original conflict level 2 into two new levels, a reduction of 5 Nm for initial d_k to 4.5 Nm, and of 1000 feet for h_k to 900 feet. Moreover for aircraft length and height values of 100 m and 40 m are assumed.

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

k	1	2	3	4	5	6	7	8
d_k	4.5 Nm	4.5 Nm	4.5 Nm	4.5 Nm	2.5 Nm	1.25Nm	0.5 Nm	100 m
h_k	900 ft	900 ft	900 ft	900 ft	900 ft	500 ft	250 ft	40 m
T_k	8 min	2.5 min	1.5 min	0 min	0 min	0 min	0 min	0 min

6.2 Two head-on flying aircraft

In this simulation two aircraft start at the same flight level, some 250 km away from each other, and fly on opposite direction flight plans head-on with a ground speed of 240 m/s.

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 5 hours on two machines, and the load of computer memory per machine was about 0.5 GigaByte. The estimated fractions $\bar{\gamma}_k^i$ are given in the table below for each of the conflict levels, k = 1,..,8.

level	1st IPS	2nd IPS	3rd IPS	4th IPS	5th IPS	6th IPS	7th IPS	8th IPS	9th IPS	10th IPS
1	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9998	1.0000	1.0000	1.0000
2	0.0003	0.0007	0.0007	0.0007	0.0005	0.0005	0.0006	0.0004	0.0003	0.0004
3	0.0000	0.0000	0.0036	0.0148	0.0000	0.0000	0.0000	0.0000	0.0143	0.0000
4	0.0000	0.0000	0.0116	0.0003	0.0000	0.0000	0.0000	0.0000	0.0031	0.0000
5	0.0000	0.0000	0.0046	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
6	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
7	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
8	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Collision Prob.	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Apparently none of the particles reaches level sets of number 6 or higher. Hence the estimated collision probability is zero. Obviously this is a very unreliable estimate of the collision risk. In other words the IPS approach does not work well for this case.

In order to estimate the collision risk for this case we used a more advanced version of IPS (studied within D9.3), the results of which are given in the following table.

level	1st Adv IPS	2nd Adv IPS	3rd Adv IPS	4th Adv IPS	5th Adv IPS	6th Adv IPS	7th Adv IPS	8th Adv IPS	9th Adv IPS	10th Adv IPS
1	0.9998	1.0000	1.0000	1.0000	1.0000	0.9996	0.9996	1.0000	1.0000	1.0000
2	0.3076	0.2848	0.2911	0.2986	0.2781	0.2903	0.2771	0.2810	0.2803	0.2975
3	0.0575	0.0483	0.0576	0.0561	0.0644	0.0422	0.0456	0.0559	0.0496	0.0539
4	0.0824	0.0625	0.0593	0.0337	0.1034	0.0719	0.0697	0.0685	0.0420	0.0648
5	0.0275	0.0184	0.0244	0.0163	0.0109	0.0231	0.0220	0.0250	0.0075	0.0433
6	0.0641	0.4296	0.2579	0.0444	0.3709	0.2675	0.4109	0.3157	0.0717	0.0964
7	0.1163	0.0427	0.0398	0.8953	0.0394	0.0466	0.0379	0.0417	0.9174	0.0581
8	0.6180	0.5792	0.5809	0.5013	0.5808	0.5849	0.5802	0.5610	0.5113	0.5879
Collision Prob.	1.84×10^{-7}	1.68×10^{-7}	1.45×10^{-7}	1.84×10^{-7}	1.72×10^{-7}	1.48×10^{-7}	1.75×10^{-7}	1.99×10^{-7}	1.47×10^{-7}	1.48×10^{-7}

The estimated mean probability of collision between the two aircraft equals 1.67×10^{-7} (i.e. the average of the bottom row values). The minimum and maximum values stay within 25% of the mean value, which shows that the estimated value is quite accurate. It is remarkable to see that the variation in the fractions per level is significantly larger than the variation in the estimated collision probability product of the fractions. Apparently, the dependency between the fractions $\bar{\gamma}_k^i$ reduces the variation in the multiplication of these fractions. This is a convincing illustration of the power of IPS for a complex hybrid state strong Markov process.

Subsequently the six main safety critical parameter values of GPS, ADS-B and ASAS were reduced by a factor 100 and the Advanced IPS was rerun. The results are given in the following Table.

level	1st Adv IPS	2nd Adv IPS	3rd Adv IPS	4th Adv IPS	5th Adv IPS	6th Adv IPS	7th Adv IPS	8thAdv IPS	9th Adv IPS	10thAdv IPS
1	0.99980	1.00000	0.99980	1.00000	1.00000	0.99980	0.99960	1.00000	0.99980	0.99980
2	0.28390	0.28290	0.29880	0.27590	0.27170	0.28180	0.28790	0.26470	0.28470	0.30240
3	0.05014	0.05007	0.05092	0.04732	0.04592	0.04097	0.05234	0.04302	0.07102	0.04323
4	0.05588	0.07256	0.05866	0.09534	0.01901	0.05170	0.05890	0.06607	0.07000	0.07676
5	0.01960	0.01696	0.02381	0.02323	0.07463	0.00768	0.02441	0.03230	0.02058	0.01837
6	0.02254	0.00016	0.45160	0.09663	0.00015	0.66030	0.20240	0.44180	0.21910	0.49690
7	0.00752	0.96180	0.00036	0.00098	0.87330	0.00114	0.00057	0.00033	0.00047	0.00032
8	0.63020	0.60500	0.58720	0.60240	0.61640	0.61480	0.58940	0.54130	0.57950	0.52390
Collision Prob.	1.66×10^{-9}	1.65×10^{-9}	2.06×10^{-9}	1.66×10^{-9}	1.43×10^{-9}	2.13×10^{-9}	1.48×10^{-9}	1.90×10^{-9}	1.72×10^{-9}	1.55×10^{-9}

The estimated mean probability of collision between the two aircraft equals 1.72×10^{-9}, i.e. a reduction by almost the same factor 100 that was applied to the six main safety critical parameter values of GPS, ADS-B and ASAS. The minimum and maximum values again stay within 25% of the mean value. This clearly shows that for this two-aircraft scenario considered, the collision risk in the model is largely caused by failures of safety critical ASAS technical systems.

6.3 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. Unfortunately with 8 aircraft the computer dynamic memory limitation allows to run IPS only.

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 load of computer memory per machine was about 2.0 GigaByte. The estimated fractions $\bar{\gamma}_k^i$ are given in the table below for each of the conflict levels, k = 1,..,8.

level	1st IPS	2nd IPS	3rd IPS	4th IPS	5th IPS	6th IPS	7th IPS	8th IPS	9th IPS	10th IPS
1	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
2	0.528	0.529	0.539	0.533	0.537	0.538	0.536	0.539	0.529	0.541
3	0.426	0.429	0.424	0.431	0.421	0.428	0.426	0.418	0.426	0.421
4	0.033	0.036	0.035	0.037	0.039	0.031	0.044	0.039	0.038	0.035
5	0.175	0.180	0.183	0.181	0.142	0.157	0.181	0.147	0.170	0.193
6	0.267	0.158	0.177	0.144	0.255	0.138	0.295	0.146	0.163	0.101
7	0.150	0.268	0.281	0.427	0.645	0.208	0.253	0.295	0.333	0.419
8	0.000	0.009	0.233	0.043	0.455	0.000	0.006	0.815	0.690	0.341
Collision Prob.	0.0	$5.58\text{x}10^{-7}$	$1.67\text{x}10^{-5}$	$4.01\text{x}10^{-6}$	$9.33\text{x}10^{-5}$	0.0	$8.00\text{x}10^{-7}$	$4.48\text{x}10^{-5}$	$5.4\text{x}10^{-5}$	$2.25\text{x}10^{-6}$

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 [Hoekstra, 2001] 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 MFF operational concept.

In practice, this particular scenario of eight aircraft, flying at the same flight level and all heading to pass the same point at the same moment in time, will rarely happen. As such it is not clear how ICAO and Eurocontrol en-route established TLS (Target Level of Safety) criteria should be applied to this eight aircraft scenario. In order to produce an estimate of collision risk for the model of the free flight operational concept for which it makes some more sense to compare it to an established TLS value, we next consider an artificial simulation of a large airspace with all kinds of encounters between multiple aircraft.

6.4 Free flight through an artificially constructed airspace with a fixed traffic density

In this simulation the complete airspace is divided into packed containers. Within each container a fixed number of seven aircraft fly at arbitrary position and in arbitrary direction at a ground speed of 240 m/s. One additional aircraft 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 neighbouring containers. In principle this can mean that an aircraft experiences a conflict with its own copy in a neighbouring 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 Nm^3. For our simulation we want a 3 times higher traffic density, i.e. 0.01 a/c per Nm^3. 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 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. The estimated fractions $\bar{\gamma}_k^i$ are given in the table below for each of the conflict levels, $k = 1,..,8$.

level	1st IPS	2nd IPS	3rd IPS	4th IPS	5th IPS	6th IPS	7th IPS	8th IPS	9th IPS	10th IPS	11th IPS
1	0.922	0.917	0.929	0.926	0.925	0.925	0.925	0.921	0.927	0.924	0.926
2	0.567	0.551	0.560	0.559	0.554	0.551	0.561	0.556	0.563	0.558	0.561
3	0.665	0.666	0.674	0.676	0.672	0.673	0.664	0.670	0.676	0.676	0.670
4	0.319	0.331	0.323	0.321	0.328	0.321	0.334	0.331	0.323	0.331	0.325
5	0.370	0.367	0.371	0.379	0.363	0.345	0.366	0.343	0.341	0.357	0.368
6	0.181	0.158	0.162	0.171	0.164	0.181	0.148	0.191	0.162	0.163	0.159
7	0.130	0.209	0.174	0.145	0.162	0.170	0.214	0.215	0.125	0.148	0.161
8	0.067	0.005	0.094	0.066	0.002	0.150	0.015	0.019	0.051	0.031	0.023
Collision Prob.	6.42×10^{-5}	6.76×10^{-6}	1.11×10^{-4}	6.99×10^{-5}	2.57×10^{-6}	1.75×10^{-4}	1.99×10^{-5}	2.98×10^{-5}	4.05×10^{-5}	3.05×10^{-5}	2.45×10^{-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? 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 [D8.4]. And once such a bias and uncertainty assessment has been performed, the bias and uncertainty corrected estimate of the risk level can be compared with the ICAO's Target Level of Safety (TLS) for mid-air collisions in en-route airspace, which currently is a maximal allowed probability of 1.5×10^{-8} collisions per aircraft flight hour. At a three times higher traffic level we assume here that this would be three times lower, i.e. 0.5×10^{-8} .Without any correction for bias and uncertainty, this is four to five orders of magnitude lower than the risk level assessed for the AMFF model. Unfortunately the current high computational load of the IPS approach prohibited the performance of such a bias and uncertainty assessment within the HYBRIDGE project. However, from past experience with bias and uncertainty assessments for collision risk models of novel air traffic operations, we

know that the bias and uncertainty of an initial simulation model differs significantly less than these four orders in magnitude.
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 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 manoeuvre by one of the two aircraft. However because of this manoeuvre there was a sudden collision with a third nearby aircraft.

These detailed evaluations of the five collision events of the 11^{th} 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 became 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 traffic in the background –as opposed to the head-on encounters in scenario 1- are the multiple conflicts. Under the far higher traffic densities then where 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.

For the current simulation results this would mean that even without having performed a bias and uncertainty assessment, our simulations for the AMFF simulation model imply the need to significantly improve the current AMFF operational concept on better handling multiple conflicts that occur under the high traffic levels considered in this section. In this respect it is good to know that there are relevant multiple conflict resolution design options, e.g. [Hoekstra, 2001], which are not exploited in the current AMFF design.

6.5 Reduction of the aircraft density by a factor four

Next 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, but 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. The estimated fractions $\overline{\gamma}_k^i$ are given in the table below for each of the conflict levels, k = 1,..,8.

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
Collision Prob.	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. Moreover, the remaining mismatch with ICAO's TLS may now fall within the applicable bias and uncertainty range. This means that the AMFF concept considered here has potential for application in traffic levels up to the current levels over Europe.

6.6 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 feasible at the start of HYBRIDGE (Blom et al, 2003a). Inherent to the IPS way of simulation, the dynamic memory of the computing machines used appeared to pose the main limitation on the full exploitation of the IPS within the period available for completing this HYBRIDGE study. 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 formally apply to the simulation model only, and need not apply to the intended AMFF operation.

The simulations performed for a model of AMFF always allow free flight operational concept developers to learn characteristics of the simulation model. Because of the IPS based speed up factor these simulations can show events that have not been observed before in Monte Carlo simulations of an AMFF model. Under far higher traffic densities then where 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 to current levels over Europe, the chance of collision for the model rapidly goes down to a level that may fall within the bias and uncertainty typically seen for an initial model of an advanced air traffic operation.

The main value of having performed this collision risk assessment 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.

7. Concluding remarks

This report presented the study performed within WP9 of the HYBRIDGE project. The main aim was to study the application of a novel method in collision risk assessment to an advanced operational air traffic management concept. First a well developed advanced free flight operation has been selected and identified for this application study. Next 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) developed in WP2 [D2.4]. Subsequently the novel IPS simulation method developed within WP8 [D8.3] has been extended for application to collision risk assessment in air traffic, and has subsequently been applied to an SDCPN model of the free flight operational concept selected.

The results obtained clearly show that the novel simulation model specification and collision risk estimation methods allow to speed up Monte Carlo simulation by orders of magnitude for a much more complex simulation model than what was possible with the state-of-the-art methods available at the beginning of the HYBRIDGE project (e.g. Blom et al., 2003a). Moreover, for the simulation model of the free flight operational concept considered, behaviour has be 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. It has also become clear that in its current form the IPS approach tends to pose very high requirements on the availability of dynamic computer memory. The good message is that WP3 has identified complementary directions in which the novel Monte Carlo simulation approach can be further developed [D3.2]. In view of this, and the fact that advanced Monte Carlo simulation currently receives a lot of research attention, it is reasonable to expect that the newly developed Monte Carlo simulation speed up approach can be further improved during follow up research.

For the further development of advanced air traffic management, the Monte Carlo simulations results lead to the following two main findings on the feasibility of using the selected operational concept at far higher traffic levels than it had been designed for:

- Further attention has to be drawn towards the development and incorporation in the particular operational concept design of advanced methods in handling multiple conflicts. [Hoekstra, 2001] studied a conflict resolution approach that performs better than the one adopted in the selected concept. Complementary to this, the HYBRIDGE developments of WP5 [D5.4] and WP6 [D6.2] have developed valuable novel complementary approaches. In addition, WP3 [D3.2] identified the need to address the roles of pilots and controllers in further studies on conflict resolution.
- The current simulations showed there are two potential sources of a too high collision risk. One potential source is the clogging of multiple conflicts. Another is the failure of safety critical technical systems. In reality there is a third one: multi-agent Situation Awareness error propagation. This will become apparent when in future we run Monte Carlo simulations of multiple conflict solution approaches that are combined with the multi-agent nature of air traffic management. In this respect the novel safety critical observation modelling and mitigation methods developed within WP7 is expected to be of use to the design of a novel free-flight concept [D7.5].

8. References

[Bakker et al, 2005] G.J. Bakker, B. Klein Obbink, M.B. Klompstra, H.A.P. Blom, DCPN specification of a free flight air traffic operation, working document, HYBRIDGE WP9.2, Version 0.5, March 2005.

[Blom et al, 2003a] H.A.P. Blom, G.J. Bakker, M.H.C. Everdij and M.N.J. van der Park, Collision risk modeling of air traffic, July 2003, ECC 2003.

[Blom et al, 2003b] H.A.P. Blom, M.B. Klompstra, G.J. Bakker, Accident risk assessment of simultaneous converging instrument approaches, Air Traffic Control Quarterly, Vol. 11, No. 2, pp. 123-155, 2003b.

[Blom et al, 2003c] 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, pp. 59-82, 2003c.

[Cerou et al, 2002] F. Cerou, P. Del Moral, F. LeGland and P. Lezaud, Genetic genealogical models in rare event analysis, Publications du Laboratoire de Statistiques et Probabilites, Toulouse III, 2002.

[D1.2] M.L. Bujorianu, J. Lygeros, W. Glover and G. Pola, A stochastic hybrid system modeling framework, HYBRIDGE D1.2 or PD2, May 2003.

[D1.4] W. Glover and J. Lygeros, Simplified Multi-Aircraft Models for Conflict Detection and Resolution Algorithms, HYBRIDGE D1.4, September 2004.

[D2.3] J. Krystul and H.A.P. Blom, Extend SDE on hybrid state space to include instantaneous jump of PDPs, HYBRIDGE D2.3 or PD10, April 2004.

[D2.4] M.H.C. Everdij and H.A.P. Blom, Modelling hybrid state Markov processes through Dynamically and Stochastically and Dynamically Coloured Petri Nets, HYBRIDGE D2.4 or PD11, September 2004.

[D3.1] M. Prandini and M.C. Campi, Reachability analysis for probabilistic hybrid systems with application to Air Traffic Management, HYBRIDGE D3.1 or PD7, November 2004.

[D3.2] M. Prandini, Probabilistic aircraft conflict detection, HYBRIDGE D3.2 or PD8, March 2005.

[D4.4] S. Strubbe, J.W. Polderman, A. Julius and A. van der Schaft, On Control of Complex Stochastic Hybrid Systems, HYBRIDGE D4.4 or PD17, April 2005.

[D5.2] A. Lecchini, W. Glover, J. Lygeros, J. Maciejowski, Model predictive control formulation of conflict resolution task, HYBRIDGE D5.2 or PD3, July 2004.

[D5.4] A. Lecchini, X. Papageorgiou, J. Lygeros, J. Majiecowski, K. Kyriakopoulos, Randomized algorithms and implementation, HYBRIDGE D5.4 or PD4, January 2005.

[D6.2] D. Dimargonas, K. Kyriakopoulos, Global decentralised conflict resolution, HYBRIDGE D6.2 or PD6, March 2005.

[D7.5] M. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, Critical observability for a class of stochastic hybrid systems and application to air traffic management, HYBRIDGE D7.5 or PD21, March 2005.

[D8.2] P. Lezaud, J. Krystul, H.A.P. Blom, Accident Risk Assessment and Monte Carlo Simulation Methods, HYBRIDGE D8.2, June 2004.

[D8.3] J.Krystul and H.A.P.Blom, Monte Carlo simulation of rare events in hybrid systems, Hybridge Report D8.3, Draft version 0.4, March 2004, http://www.nlr.nl/public/hosted-sites/hybridge/

[D8.4] M.H.C. Everdij and H.A.P. Blom, Bias and uncertainty modelling in accident risk assessment, HYBRIDGE D8.4 or PD14, February 2005.

[D9.1] B.Klein Obbink, Description of advanced operatation: Free flight, HYBRIDGE D9.1, March 2005.

[D9.2] M.H.C. Everdij, M.B. Klompstra, H.A.P. Blom, B. Klein Obbink, Compositional specification of a multi-agent system by Dynamically Coloured Petri Nets, HYBRIDGE D9.2, 22 November 2004, Version 0.5

[D9.3] J. Krystul, H.A.P. Blom, Sequential Monte Carlo simulation of rare event probability, HYBRIDGE D9.3, 21st December 2004.

[DAG-TM] 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.

[David & Alla, 1994] R. David, H. Alla, Petri Nets for the modeling of dynamic systems - A survey, Automatica, Vol. 30, No. 2, pp. 175-202, 1994.

[Del Moral 2003] P. Del Moral, Feynman-Kac Formulae. Genealogical and Interacting Particle Systems with Applications, Springer, 2004.

[Doucet et al, 2001] A. Doucet, N. de Freitas and N.Gordon, Sequential Monte Carlo Methods in Practice, Springer-Verlag, 2001.

[Erzberger, 2004] H.Erzberger, Transforming the NAS: The next generation air traffic control system, Proc. 24th Int. Congress of the Aeronautical Sciences (ICAS 2004).

[Everdij and Blom, 2002] 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.

[Everdij & Blom, 2003a] M.H.C. Everdij, H.A.P. Blom, Piecewise Deterministic Markov Processes represented by Dynamically Coloured Petri Nets, NLR-TP-2000-428, National Aerospace Laboratory NLR, Revised edition, 2003a.

[Everdij & Blom, 2003b] M.H.C. Everdij, H.A.P. Blom, Petri Nets and Hybrid state Markov Processes in a power-hierarchy of dependability models, Proc. IFAC Conference on Analysis and Design of Hybrid Systems, Saint-Malo Brittany, France, pp. 355-360, June 2003b. Preprint available on http://www.nlr.nl/public/hosted-sites/hybridge/

[Fernandes et al, 1997] M. Fernandes, M. Adamski, and A.J. Proença. VHDL Generation from Hierarchical Petri Net Specifications of Parallel Controller. IEE Proceedings: Computers and Digital Techniques, Vol. 144, pp. 127-137, March 1997.

[FFlit] Free flight research issues and literature search. Under NASA contract NAS2-98005, J. Krozel, 2000.

[Fleischhack & Grahlmann, 1997] H. Fleischhack, B. Grahlmann, A Petri net semantics for $B(PN)^2$ with procedures, Parallel and Distributed Software Engineering, 1997.

[Fota et al, 1997] N.O. Fota, M. Kaaniche and K. Kanoun, A modular and incremental approach for building complex stochastic Petri net models, Proc. First Int. Conf. on Mathematical Methods in Reliability, 1997.

[Glasserman 2003] Glasserman, P., Monte Carlo Methods in Financial Engineering, Stochastic Modelling and Applied Probability, Vol. 53, Springer, 2003.

[Haas, 2002] P.J. Haas, Stochastic Petri Nets, Modelling, Stability, Simulation, Springer-Verlag, New York, 2002.

[Harel, 1987] D. Harel, Statecharts: a visual formalism for complex systems. Science of Computer Programming, Vol. 8, pp. 231-274, 1987.

[Hoekstra, 2001] J. Hoekstra, Designing for Safety, the Free Flight Air Traffic Management concept, PhD Thesis, Delft University of Technology, November 2001.

[Huber et al, 1990] P. Huber, K. Jensen, R.M. Shapiro, Hierarchies in Coloured Petri Nets, G. Rozenberg (ed.): Advances in Petri nets 1990. Lecture notes in Computer Science, Vol. 483. Springer, Berlin Heidelberg New York 1990, pp. 313-341.

[Hybridge Project] Hybridge Project Management Plan, WP0, Version 0.2, HYBRIDGE/NLR/WP0/PMP/0.2, March 2002.

[ICAO ASAS Circ] ICAO circular on airborne separation assistance system (ASAS).

[Kindler, 1997] D. Kindler, A compositional partial order semantics for Petri net components, 18th International Conference on Application and Theory of Petri nets, Pierre Azema and Gianfranco Balbo (ed.), LNCS, 1248, Springer-Verlag, June 1997.

[Krystul & Blom, 2004] J. Krystul and H.A.P. Blom, Sequential Monte Carlo simulation of rare event probability in stochastic hybrid systems, IFAC05, submitted, September 2004.

[Labeau et al, 2000] P.E. Labeau, C. Smidts and S. Swaminathan (2000). Dynamic reliability: towards an integrated platform for probabilistic risk assessment. Reliability Engineering and System Safety 68, 219-254.

[PO-ASAS] Principles of Operations for the Use of ASAS, Action Plan 1 FAA/Eurocontrol Cooperative R&D, Version 7.1, 2001.

Appendix A Acronyms

ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependent Surveillance Broadcast
AMFF	Autonomous Mediterranean Free Flight
ASAS	Airborne Separation Assurance System
ATC	Air Traffic Control
ATM	Air Traffic Management
$B(PN)^2$	Basic Petri Net Programming Notation
CDTI	Cockpit Display of Traffic Information
CPN	Coloured Petri Nets
DCPN	Dynamically Coloured Petri Net
DME	Distance Measuring Equipment
FFAS	Free Flight AirSpace
FMS	Flight Management System
GNSS	Global Navigation Satellite System
GPS	Satellite Navigation and Global Positioning System
GSPNs	Generalized Stochastic Petri nets
ICAO	International Civil Aviation Organisation
IFR	Instrument Flight Rules
INS/IRS	Inertial Navigation and Inertial Reference Systems
IPN	Interaction Petri Net
IPS	Interacting Particle System
LPN	Local Petri Net
MC	Monte Carlo
MFF	Mediterranean Free Flight
M-nets	modular multilabelled nets
NDB	Non-Directional Beacon

R/T	Radio/Telecommunication
SA	Situation Awareness
SDCPN	Stochastically and Dynamically Coloured Petri Net
SDE	stochastic differential equation
SIPN	Synchronous Interpreted Petri Nets
TLS	Target Level of Safety
VOR	VHF Omni-directional Radio Range (Beacon)