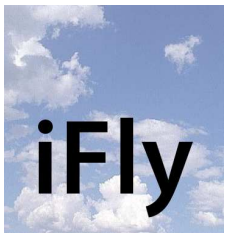

Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

iFly

Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management

Specific Targeted Research Projects (STREP)

Thematic Priority 1.3.1.4.g Aeronautics and Space

iFly Deliverable D7.4

Final Report on Accident Risk Assessment of the A^3 operation

Version: 0.7

H.A.P. Blom and G.J. Bakker
NLR

Due date of deliverable: 22 January 2011
Actual submission date: 30 September 2011

Start date of project: 22 May 2007 Duration: 51 months

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

DOCUMENT CONTROL SHEET

Title of document:	*Final Report on Accident Risk Assessment of the A³ operation*
Authors of document:	*H.A.P. Blom and G.J. Bakker*
Deliverable number:	*D7.4*
Project acronym:	*iFly*
Project title:	*Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management*
Project no.:	*TREN/07/FP6AE/S07.71574/037180 IFLY*
Instrument:	*Specific Targeted Research Projects (STREP)*
Thematic Priority:	*1.3.1.4.g Aeronautics and Space*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
0.1	28 June 2011	All	First draft
0.2	15 July 2011	All	Second draft
0.3	28 July	All	Third draft
0.4	31 July	References	Intermediate report
0.5	19 August	Sections 5-7	New simulation results
0.6	31 August	Sections 4-7	Edit cycle
0.7	19 September	All	Internal review incorporated

Authors	H.A.P. Blom	NLR	
	G.J. Bakker	NLR	
Internal reviewers	M.B. Klompstra	NLR	
External reviewers			

Abstract

In WP1 of the iFLY project, an advanced airborne self separation design has been developed under the name A^3 ConOps (Concept of Operations). The aim of the current D7.4 report is to perform an assessment of this A^3 operation on accident risk as a function of en-route traffic demand, including sensitivity analysis. This way it should become clear what factor more traffic than in 2005 can safely be accommodated by the A^3 advanced operational concept. The accident risk assessment is conducted using advanced techniques in Agent Based Modelling and Rare Event Monte Carlo simulation. The results obtained show that under the A^3 ConOps, very high en-route traffic demand can safely be accommodated.

Table of Contents

Acronyms

Acronym	Definition
A^3	Autonomous Aircraft Advanced
a/c	Aircraft
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependant Surveillance - Broadcast
AFR	Autonomous Flight Rules
AMFF	Autonomous Mediterranean Free Flight
ANP	Actual navigation performance
ANSP	Air Navigation Services Provider
AOC	Airline Operations Centre
ASAS	Airborne Separation Assistance System
ATM	Air Traffic Management
CD	Conflict Detection
CD&R	Conflict Detection and Resolution
CDTI	Cockpit Display of Traffic Information
CNS	Communication, Navigation & Surveillance
ConOps	Concept of Operations
CR	Conflict Resolution
CTA	Controlled Time of Arrival
DCPN	Dynamically Coloured Petri Net
E-OCVM	European Operational Concept Validation Methodology
FMS	Flight Management System
GNC	Guidance, Navigation and Control
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSHS	General Stochastic Hybrid System
HHIPS	Hierarchical Hybrid IPS
ICAO	International Civil Aircraft Association
IPN	Interaction Petri Net
IPS	Interacting Particle System
IRS	Inertial Reference System
LOS	Loss of Separation
LPN	Local Petri Net
MAC	Mid-Air Collision
MC	Monte Carlo
MSI	Minimum Separation Infringement
MTC	Medium Term Conflict
MTCR	Medium Term Conflict Resolution
n.a.	not applicable
Nm	Nautical mile
NMAC	Near Mid-Air Collision
OSED	Operational Services and Environmental Description
P-ASAS	Predictive Airborne Separation Assurance System

Acronym	Definition
PBC	Periodic Boundary Condition
PF	Pilot Flying
PNF	Pilot Non-Flying
RBT	Reference Business Trajectory
RNP1	Required Navigation Performance of 1 NM
RTD	Research, Technology and Development
SA	Situation Awareness
SDCPN	Stochastically and Dynamically Coloured Petri Net
SESAR	Single European Sky ATM Research
SMC	Sequential MC
SSA	Self Separation Airspace
STC	Short Term Conflict
STCR	Short Term Conflict Resolution
SWIM	System Wide Information Management
TCAS	Tactical Collision Avoidance System
TCP	Trajectory Change Point
TLS	Target Level of Safety
TMA	Terminal Area
TOPAZ	Traffic Organization and. Perturbation AnalyZer
WP	Work Package

1 Introduction

1.1 Key research objective

Air transport throughout the world, and particularly in Europe, is characterised by major capacity, efficiency and environmental challenges. With the predicted growth in air traffic, these challenges must be overcome to improve the performance of the Air Traffic Management (ATM) system. The air traffic capacity/safety wall has to be moved by a large factor in order to meet the growing demand for business and recreational travel without sacrificing established (very high) safety standards. The conventional approach of air traffic controllers being responsible for the safe and expeditious flow of air traffic in their sectors appears to have reached its limits. Hence the air transport industry is in need of developing a novel paradigm that indeed is able to significantly push the capacity/safety barrier. One of the most innovative and promising paradigm is to transfer the responsibility of maintaining separation with other aircraft from sector air traffic controllers to the pilots of each aircraft. In short, we refer to such a complete transfer of separation responsibility as airborne self separation. Since the invention of Free Flight [RTCA, 1995] airborne self separation research has seen a tremendous development worldwide. Nevertheless, the current situation is of two schools of researchers holding different beliefs about airborne self separation:

- One school believes airborne self separation can be performed at sufficiently safe levels en-route and at traffic levels well above the current situation;

- The other school believes airborne self separation cannot be carried out at sufficiently safe levels above Europe.

In fact these two opposite schools also agree on two key points:

1. For low traffic airspace areas the safety will be improved by equipping aircraft with the appropriate Airborne Separation Assistance System (ASAS); which resulted in a steady development and implementation of airborne self separation operations in some low traffic airspace areas around the world;

2. None of the schools exactly knows at which traffic levels the safety/capacity barrier of airborne self separation lies. Hence both schools are in need of receiving an answer to the question “At what traffic level the safety of advanced airborne self separation based operation falls short?”

Without having a proper answer to the latter question, there is large uncertainty to the strategic direction to be taken regarding the further development of airborne self separation, and this may even tend to stall its further development. Even worse, this may have negative impact on the development referred to under 1, although the two schools do not differ. The very reason is that investments by airlines in an advanced system that can be used in airspace where their aircraft hardly fly is economically very unattractive. Hence both for developments 1 and 2 there is an urgent socio-economic need for the aviation industry to know how far airborne self separation can safely support increasing traffic demands.

From a societal perspective, citizens expect air transport to be affordable and safe in the future as well as it is now. Hence, a potential stall or delay in the further investment by the air

transport industry into airborne self separation, eventually may have a very negative impact on the users of the air transport system, and thus on human society. Hence it is human society that benefits significantly from a continuation of effective strategic investments of the aviation industry into advanced air traffic operations. A key condition which has to be fulfilled is that the two schools are able to present a joint view to the air transport industry. iFly aims to develop the key missing scientific pieces of knowledge that solve the puzzles of both schools, this means that iFly frees the ASAS developments from this very expensive stall, and makes rationale investments into strategic development of ASAS possible again.

1.2 iFly project

The iFly project will develop and assess an advanced airborne self separation Concept of Operation for en-route traffic, which is aimed to manage a three to six times as high traffic demand than high traffic demand in 2005.

iFly will perform two operational concept design cycles and an assessment cycle comprising human factors, safety, efficiency, capacity and economic analyses. The general work structure is illustrated in Figure 1. During the first design cycle, state of the art Research, Technology and Development (RTD) aeronautics results will be used to define a "baseline" operational concept. For the assessment cycle and second design cycle, innovative methods for the design of safety critical systems will be used to refine the operational concept with the goal of managing a three to six times increase in traffic demand of 2005. These innovative methods find their roots in robotics, financial mathematics and telecommunications.

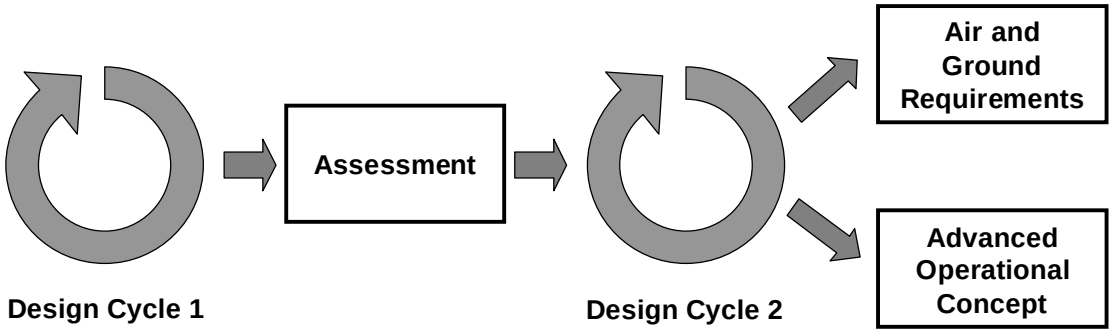

FIGURE 1. iFly Work Structure.

As depicted in Figure 2, iFly work is organised through nine technical Work Packages (WPs), each of which belongs to one of the four types of developments mentioned above:

Design cycle 1

The aim is to develop an Autonomous Aircraft Advanced (A^3) en-route operational concept which is initially based on the current "state-of-the-art" in aeronautics research. The A^3 ConOps is developed within WP1. An important starting and reference point for this A^3 ConOps development is formed by the human responsibility analysis in WP2.

Innovative methods

Develop innovative architecture free methods towards key issues that have to be addressed by an advanced operational concept:

- Develop a method to model and predict complexity of air traffic (WP3).
- Model and evaluate the problem of maintaining multi-agent Situation Awareness (SA) and

avoiding cognitive dissonance (WP4).
- Develop conflict resolution algorithms for which it is formally possible to guarantee their performance (WP5).

Assessment cycle

Assess the state-of-the-art in Autonomous Aircraft Advanced (A^3) en-route operations concept design development with respect to human factors, safety and economy, and identify which limitations have to be mitigated in order to accommodate a three to six times increase in air traffic demand:
- Assess the A^3 operation on economy, with emphasis on the impact on organisational and institutional issues (WP6).
- Assess the A^3 operation on safety as a function of traffic density increase over current and mean density level (WP7).

Design cycle 2

The aim is to refine the A^3 ConOps of design cycle 1 and to develop a vision how A^3 equipped aircraft can be integrated within SESAR concept thinking (WP8). WP9 develops preliminary safety and performance requirements on the applicable functional elements of the A^3 ConOps, focused on identifying the required technology.

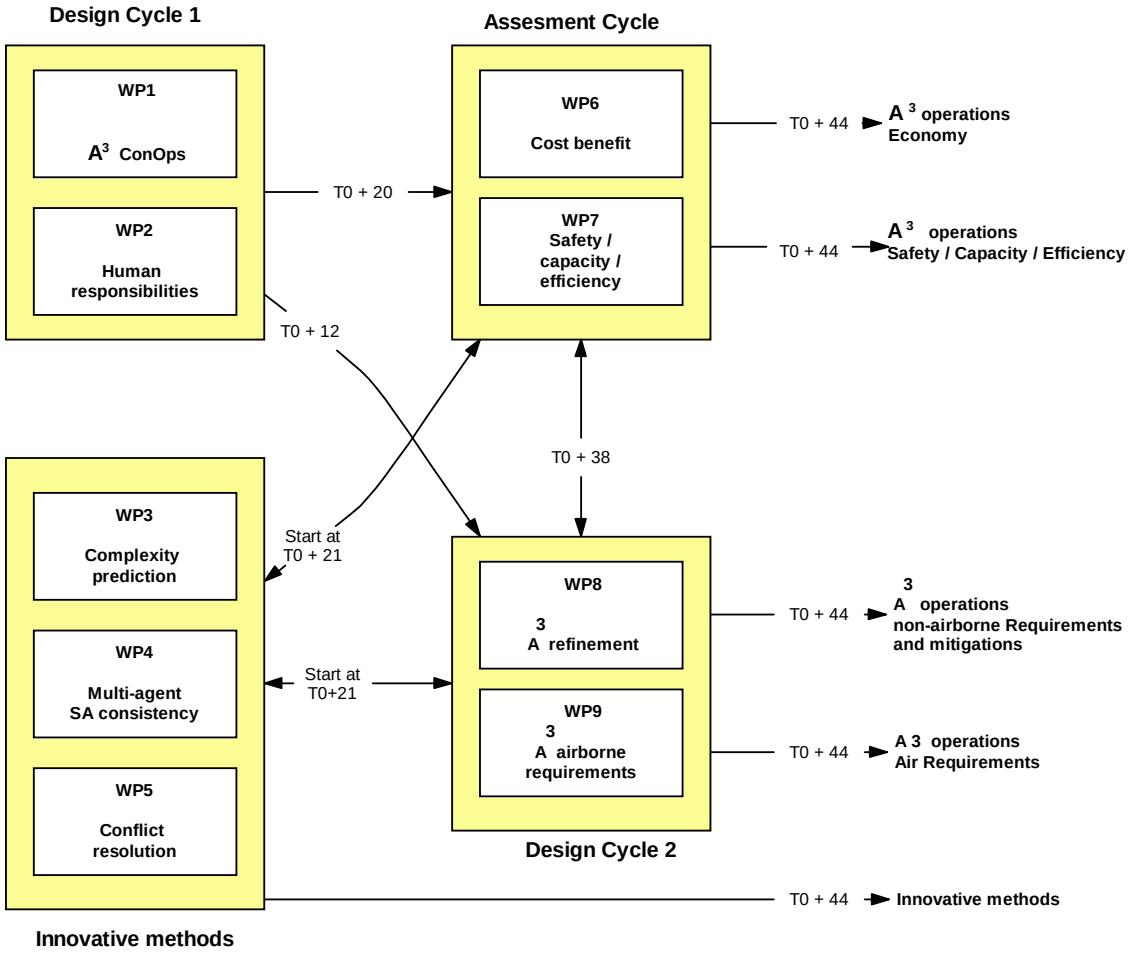

FIGURE 2. Organisation of iFly research.

1.3 Objective of iFly work package 7

The objective of iFly WP7 is to assess the Autonomous Aircraft Advanced (A^3) operations developed by WP1 (A^3 Concept) and WP2 (Human responsibilities in autonomous aircraft operations), through hazard identification and Monte Carlo simulation on accident risk as a function of traffic demand, to assess what traffic demand can safely be accommodated by this advanced operational concept. In order to accomplish this assessment through Monte Carlo simulation, the complementary aim of this WP is to further develop the innovative HYBRIDGE speed up approaches in rare event Monte Carlo simulation. The work is organised in three streams:

- Stream 1: Monte Carlo simulation model of the A^3 ConOps;
- Stream 2: Monte Carlo speed up methods;
- Stream 3: Assess the A^3 ConOps under very high traffic demands.

1.4 Stream 1: Monte Carlo simulation model of A^3 operation

The development of a Monte Carlo simulation model of A^3 operation is accomplished through a sequence of steps. First, a scoping has been performed regarding the desired risk and capacity simulation study. An important aspect of this scoping is to identify the appropriate safety requirements to be derived from safety regulation. This has been reported in [iFly D7.1a]. Then, a hazard identification and initial hazard analysis has been performed for the A^3 operation as has been developed by WP1 and WP2 [iFly D1.3, iFly D2.2]. This has been reported in [iFly D7.1b]. In parallel to the initial hazard analysis, the development of a Monte Carlo simulation model has been started that aims to capture the accident risk and the flight efficiency of the A^3 operation. Such a simulation model covers the human and technical agents, their interactions and both the nominal and non-nominal aspects of the operation. This has been reported in [iFly D7.1c].

1.5 Stream 2: Monte Carlo speed up methods

Within HYBRIDGE novel Monte Carlo simulation speed up techniques have successfully been developed and applied. In [iFly D7.2a] a review has been provided of the Monte Carlo simulation based accident risk assessment situation. Subsequently, the following directions have been investigated for the development of complementary speed-up and bias and uncertainty assessment techniques:

- To combine Interacting Particle System based rare event simulation with Markov Chain Monte Carlo speed up technique. This has been reported in [iFly D7.2b].
- To study the sensitivity of multiple aircraft encounter geometries to collision risk, and develop importance sampling approaches which take advantage of these sensitivities. This has been reported in [iFly D7.2c].
- To study ways how Interacting Particle System speed up techniques that apply to a pair of aircraft can effectively be extended to situations of multiple aircraft. This has been reported in [iFly D7.2d].
- To extend Interacting Particle System based rare event simulation for application to hybrid systems. This has been reported in [iFly D7.2e].

- To study Monte Carlo simulation based bias and uncertainty assessment with operation design parameter optimization. This has been reported in [iFly D7.2f].

Finally, in [iFly D7.2g] it has been reported how the above developments have been used for the safety risk assessment of the A^3 ConOps in stream 3.

1.6 Stream 3: Assess the A^3 ConOps under very high traffic demands

In this stream, rare event Monte Carlo simulations are performed to assess collision risk of the A^3 operation. The rare event MC simulations include sensitivity analysis, and a comparison of the assessed risk level against the applicable future Target Level of Safety (TLS) that has been derived in [iFly D7.1a]. The current report documents the results obtained within this third stream.

1.7 Organisation of this report

This report is organised as follows. Section 2 introduces the A^3 operation considered. Section 3 presents a high level view of the developed multi-agent model using the Petri net formalism. Section 4 addresses how the A^3 model is used to realize MC simulation of the A^3 operation. Sections 5-7 present the rare event MC simulation results obtained for three encounter types. Section 8 presents conclusions.

2 Introduction to the A^3 ConOps

2.1 Background

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), and led to the proposal of airborne self separation as a potential solution towards accommodating significantly higher traffic demands than conventional ground based air traffic control [RTCA, 1995]. With support from adequate decision-support tools, aircraft crew should be able to assure safe separation without the need for receiving tactical instructions from an air traffic controller, and air traffic controller's workload should no longer constitute a limiting factor in accommodating traffic growth.

In [RTCA, 1995] it also has been proposed that aircrew obtain the freedom to select their trajectory, and the conceptual idea has been called free flight. Airborne self separation 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. 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 many aircraft potentially involved, the system is highly distributed. Since the initial free flight concept definition leaves open many challenges in developing adequate procedures, systems and regulations, it has motivated the study of multiple airborne self separation operational concepts, implementation choices and requirements, e.g. [Duong & Hoffman, 1997; NASA, 1999, 2004; Krozel, 2000; Hoekstra, 2001; FAA/Eurocontrol, 2001; ICAO, 2003].

All these concepts make use of an Airborne Separation Assistance System (ASAS) onboard an aircraft. Key differences concern the coordination assumed between the aircraft, and whether all aircraft are equipped or not. Both [Duong & Hoffman, 1997] and [Hoekstra, 2001] assume all aircraft to be ASAS equipped which supports pilots with some implicit form of coordination in tactical conflict resolution only. A full ConOps for the latter approach has been developed to accommodate air traffic over the Mediterranean area [Gayraud et al., 2005], [Maracich, 2005]. [Blom, ATC-Q2009] refers to this ConOps as Autonomous Mediterranean Free Flight (AMFF) and shows that this ConOps falls short in safely accommodating high demands of en-route traffic. The main reason is that, under high traffic demand, the AMFF specific form of implicit coordination tends to create almost as many conflicts as it solves [Blom, ATC-Q2009]. In [NASA, 2004] an airborne self separation high level concept has been proposed where ASAS conflict resolution is assumed to work both strategically and tactically, including some implicit form of coordination such as priority rules. In contrast with AMFF, this NASA concept also allows mixed airborne equipment in the sense that non-equipped aircraft are assumed to be supported by air traffic control. If we exclude this mixed equipment capability, then the A^3 ConOps developed in [iFly D1.3] has a lot in common with the high level concept of [NASA, 2004] under the hypothetical situation of 100% well equipped aircraft. For further details of the A^3 ConOps and A^3 Operational Services and Environmental Description (OSED), see [iFly D1.3] and [iFly D9.1]. Here we give a high level description of the A^3 intended operation only.

2.2 A³ operation

Under the A³ ConOps, a typical airborne self separation flight may have the following progression. When an aircraft takes off from an airport it first climbs through a Terminal Manoeuvring Area (TMA), where the traffic flow is controlled by the Air Navigation Service Provider (ANSP) who is responsible for aircraft separation. Already at that moment in time for each flight there is an agreed and shared flight trajectory plan (referred to as Reference Business Trajectory (RBT)) up to the destination allowing to balance the capacity/demand en-route and at the destination TMA and airport. For this purpose there is a flow constraint associated to the flight at the entering fix of the destination TMA in the form of a 3D point with a Constrained Time of Arrival (CTA) restriction.
From the moment that the aircraft leaves the TMA, it enters the en route Self Separation Airspace (SSA), and the responsibility for separation is shifted from the ANSP to the flight crew. Once being within SSA, the flight crew can modify the SSA-part of the RBT without negotiation with any ANSP, provided that defined Autonomous Flight Rules (AFR) are satisfied and that the CTA at the destination TMA will be achieved. In case there is a need to modify the current CTA constraint, then the change must be negotiated with the ANSP of the destination TMA. In SSA the aircraft need not follow any predefined airway structure. When the aircraft approaches the destination TMA, the responsibility for separation is shifted back from the flight crew to the ANSP and the self-separation part of the flight is terminated.
According to the A³ ConOps, within SSA information exchange between aircraft is assured through datalink. Voice communication will be limited and mainly for use under emergency situations. When flying in SSA, each aircraft is obliged to broadcast information about its state and intent to the other aircraft. This allows each aircraft to predict the intended trajectories of all aircraft, and to act such that minimum separation criteria are not violated. Coordination of actions by conflicting aircraft is done in line with the AFR, which are binding to all participants. The A³ ConOps also foresees that aircraft that cannot be reached by broadcasting receive the missing information through a System Wide Information Management (SWIM) network.
In order to ensure separation and onboard trajectory management tasks, the flight crew takes advantage of the onboard equipment, which is monitoring the surroundings and helps the flight crew to detect and resolve conflicts. The onboard equipment supports two lines of defence in the timely resolution of potential conflicts: Medium Term Conflict Resolution (MTCR) and Short Term Conflict Resolution (STCR).
The time horizon for MTCR lies 15-20 minutes ahead of potential infringement of minimum separation between planned trajectories. When a Medium Term Conflict between two aircraft is detected, then the aircraft having lowest priority has to resolve the conflict. The aircraft with higher priority simply continues to fly its original trajectory. The priority of an aircraft evolves during the flight and is primary determined by the aircraft manoeuvrability, mission statement and the remaining time to CTA. The lower priority aircraft should adapt its RBT in order to solve the conflict as well as not creating a conflict with any of the other aircraft RBT's. Ideally, all conflicts should be solved through the Medium Term Conflict Resolution line of defence. When the MTCR equipment proposes a change in the intent, it first has to be approved by the flight crew, then its own RBT is updated and then the aircraft broadcast their new intent to other aircraft.
When the MTCR line of defence is not able to solve the conflict then the next line of defence is STCR. The time horizon for STCR lies 5 minutes ahead of potential infringement of minimum separation criteria. When such an event is detected, then no priority exists and all aircraft involved have to manoeuvre The applied manoeuvres shall be coordinated through implicit coordination, which means the use of compatible algorithms that generate

complementary manoeuvres when used by involved conflicting aircraft. In case this second line of defence does not timely resolve all potential conflicts, then TCAS forms the third line of defence.

2.3 ASAS relevant elements

The ASAS relevant elements in the A^3 ConOps design can be summarized as follows:

- All aircraft are supposed to be A^3 equipped, and their ADS-B periodically broadcasts own aircraft state and intent information, and periodically receives the state and intent information messages broadcasted by other aircraft.

- 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.

- ASAS related information is presented to the crew through a Cockpit Display of Traffic Information (CDTI).

- Following [iFly D1.3], the aim is to work with a vertical separation minimum of 900 ft and with a horizontal separation minimum of 3Nm (which is referred to as Minimum Separation Zone). A conflict is detected if these separation minima will be violated within medium term or short term horizon. Minimum separation between centre lines of intents are 1000 ft and 5Nm in vertical and horizontal direction respectively (which is referred to as Comfort Separation Zone).

- The conflict resolution process consists of two phases: MTCR and STCR. During the MTCR phase, one of the aircraft crews should make a resolution maneuver. If this does not work, then during the STCR phase, both crews should make a resolution maneuver.

- Both STCR and MTCR are intent-based, i.e. available intent information of own and other aircraft is taken into account when identifying a conflict free RBT. A key difference between MTCR and STCR is that the former uses priority rules and the latter not.

- During STCR, co-ordination does not take place explicitly, i.e., there is no communication on when and how a resolution maneuver will be executed.

2.4 Velocity Obstacles based conflict detection and resolution

The review in [iFly D8.1] of literature sources and the results of WP5 [iFly D5.3] show there are a large variety of conflict detection and resolution approaches available for potential use within the A^3 ConOps. In order to perform a risk assessment using rare event Monte Carlo simulation, one of these approaches had to be selected. Because computational load is a severe issue in rare event Monte Carlo simulation, we have selected Conflict detection and resolution approaches which are mathematically sound, though without requiring a high computational load. In view of these two criteria, Velocity Obstacles based conflict detection and resolution [Fiorini & Schiller, 1998], [Abe & Yoshiki, 2001] has been identified as a good safety analysis directed choice for use within the A^3 ConOps. Within the ASAS context,

Velocity Obstacles based conflict detection and resolution means that an aircraft stays away from the set of courses and velocities that lead to a predicted conflict with any other aircraft. In airborne self-separation research, this Velocity Obstacles approach has been referred to as Predictive ASAS [Hoekstra, 2001].

Figure 3 shows a 10 minutes Medium Term Velocity Obstacle area that applies for the aircraft at left, in case of a head on encountering aircraft at a distance of about 140 Nm. The red line shows for the left hand aircraft a trajectory plan which is conflict free 15 minutes ahead.
Figure 4 shows that this Medium Term Velocity Obstacle area only doubles when there are six more aircraft that are encountering on collision courses. Again the red line shows for the left hand aircraft a trajectory plan which is conflict free 15 minutes ahead.
Figure 5 shows that the Medium Term Velocity Obstacle area becomes significantly larger in case of five head on aircraft. And again the red line shows for the left hand aircraft a conflict free trajectory plan.
Figure 6 shows what the 3 minutes Short Term Velocity Obstacle area becomes in case the encounter condition in Figure 5 remains unchanged until 3 minutes prior to conflict. The total area of the Velocity Obstacle is now much smaller than in Figure 5 thanks to two effects:

1) Prediction horizon is 3 minutes rather than 10 minutes; and
2) Separation criterion is now 3 Nm rather than the 5 Nm of the Medium Term horizon.

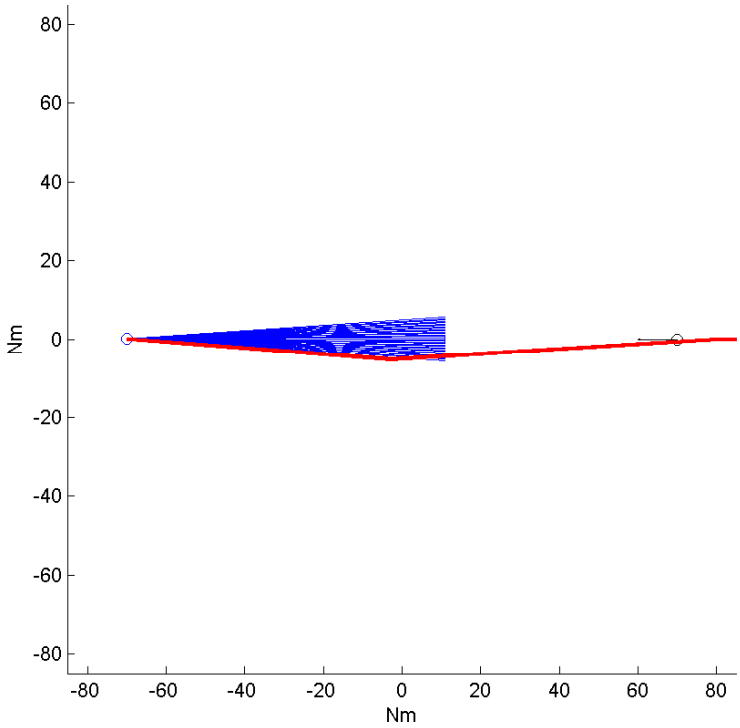

FIGURE 3: Medium Term Velocity Obstacle (10 minutes & 5 Nm.) for one head-on encountering aircraft, at the same flight level.

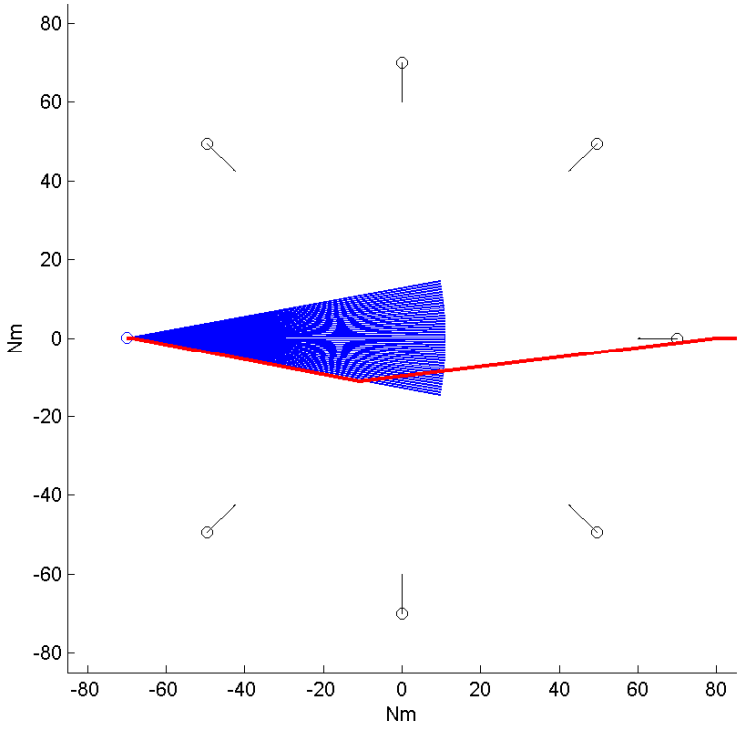

FIGURE 4: Medium Term Velocity Obstacle (10 minutes & 5 Nm.) for seven encountering aircraft from several directions, at the same flight level.

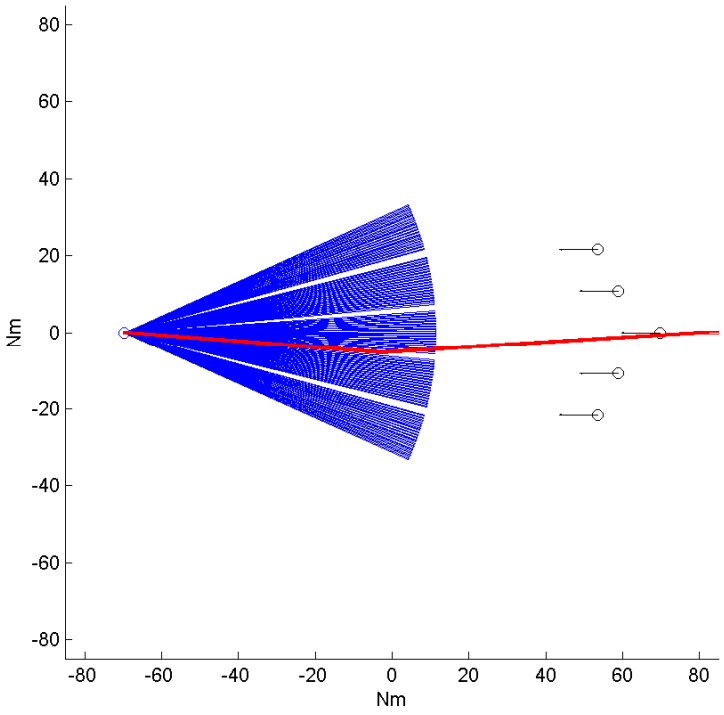

FIGURE 5: Medium Term Velocity Obstacles (10 minutes & 5 Nm.) for five head-on encountering aircraft, at the same flight level.

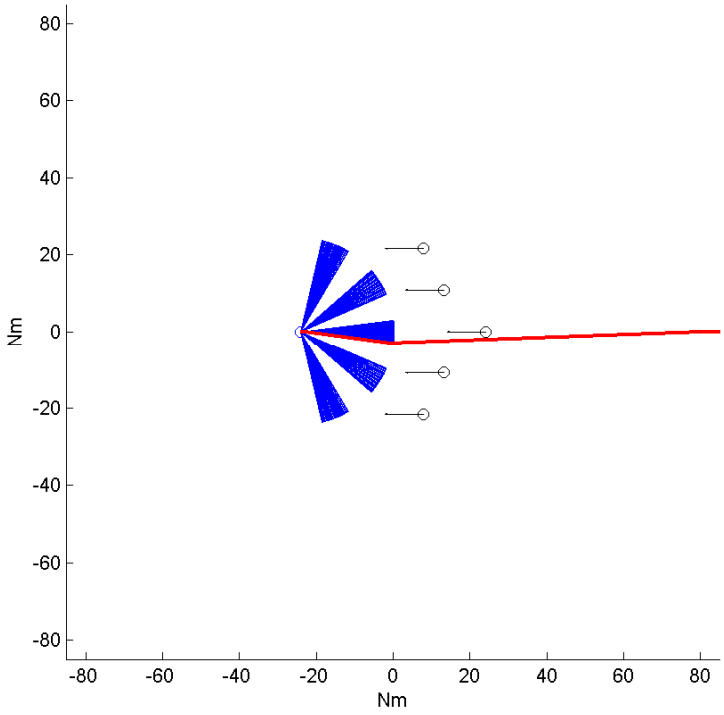

FIGURE 6: Short Term Velocity Obstacles (3 minutes & 3 Nm.) in case the five encountering aircraft situation of Figure 5 has remained unresolved.

3 A³ ConOps model

This section provides an overview of the agent based modelling of the A³ Operation. The mathematical modelling language used for this is the framework of Stochastically and Dynamically Coloured Petri Nets (SDCPN). Appendix A explains this SDCPN formalism.

3.1 Agents in A³ model

In the A³ model the following types of agents are taken into account:

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

It should be noticed that this A³ model is an initial one which does not (yet) incorporate environment/weather, Airborne Collision Avoidance System (ACAS) or Airline Operations Centre (AOC). Moreover, our current ASAS model is restricted to horizontal conflict detection and resolution, which implies that for the time being only aircraft flying at the same flight level are considered.

The Petri net formalism supports a compositional specification approach, which means that first for each agent particular local Petri nets are being developed using agent specific expert knowledge, and without the need to bother about the connections between the agents. Once this has been done, the interactions between these local Petri nets are being developed. A listing of local Petri nets per agent is given in Table 1.

TABLE 1. Agents and local Petri nets in the A³ model

- Aircraft state local Petri nets:
  - Type
  - Engine system mode
  - Navigation system mode
  - Emergency mode
- Pilot-Flying (PF) local Petri nets:
  - State Situation Awareness
  - Intent Situation Awareness
  - Goal memory
  - Current goal
  - Task performance
  - Cognitive mode
- Pilot-Not-Flying (PNF) local Petri nets:
  - Current goal
  - Task performance
- Airborne GNC local Petri nets:
  - 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
  - Guidance mode
  - Horizontal guidance configuration mode
  - Vertical guidance configuration mode
  - FMS Intent
  - Airborne GPS receiver
  - Airborne Inertial Reference System (IRS)
  - Altimeter
  - Horizontal position processing
  - Vertical position processing
  - Regular Broadcast FMS Intent
  - ADS-B transmission
  - ADS-B receiver
- ASAS local Petri nets:
  - Surveillance
  - State & Intent other aircraft
  - Conflict Detection & Management
  - Resolution Mode
  - STCR Advisory
  - MTCR Advisory
  - STC Audio alerting
  - MTC Audio alerting
  - Conformance Monitoring Intent other aircraft
  - System mode
- Communication / Navigation / Surveillance systems local Petri nets:
  - Global Navigation Satellite System (GNSS)
  - Global ADS-B ether frequency
  - SSR Mode-S frequency

The resulting A^3 model comprises 43 different local Petri nets. For each Agent, except for the last one, all local Petri nets are copied for each aircraft in the A^3 model. Hence, for N aircraft, there are 40N+3 local Petri nets in the A^3 model.

3.2 Interconnected LPNs of ASAS

This subsection illustrates the Petri Net model developed for ASAS onboard each aircraft.
ASAS for aircraft *i* is modelled through the SDCPN depicted in Figure 7. The ADS-B information received from other aircraft is processed by the *LPN ASAS surveillance*. This yields estimates of the state and intent of all other aircraft which are maintained in the *LPN ASAS State & Intent other a/c*. This LPN also maintains other relevant information for each other a/c, such as mode, priority and handycap information.
Together with the information about its own aircraft state information (from Airborne GNC agent), this information is used by *LPN ASAS CD & Management* to detect conflicts of a/c *i* with any of the other aircraft. The *LPN ASAS Resolution Mode* determines which type of conflict advice should be provided to the crew. The *LPN STCR Audio Alert* and *LPN MTCR Audio Alert* send a corresponding audio alert signal to the crew. The *LPN STCR Advisory* and *LPN MTCR Advisory* determine the advisory to be provided to the crew of aircraft *i*.

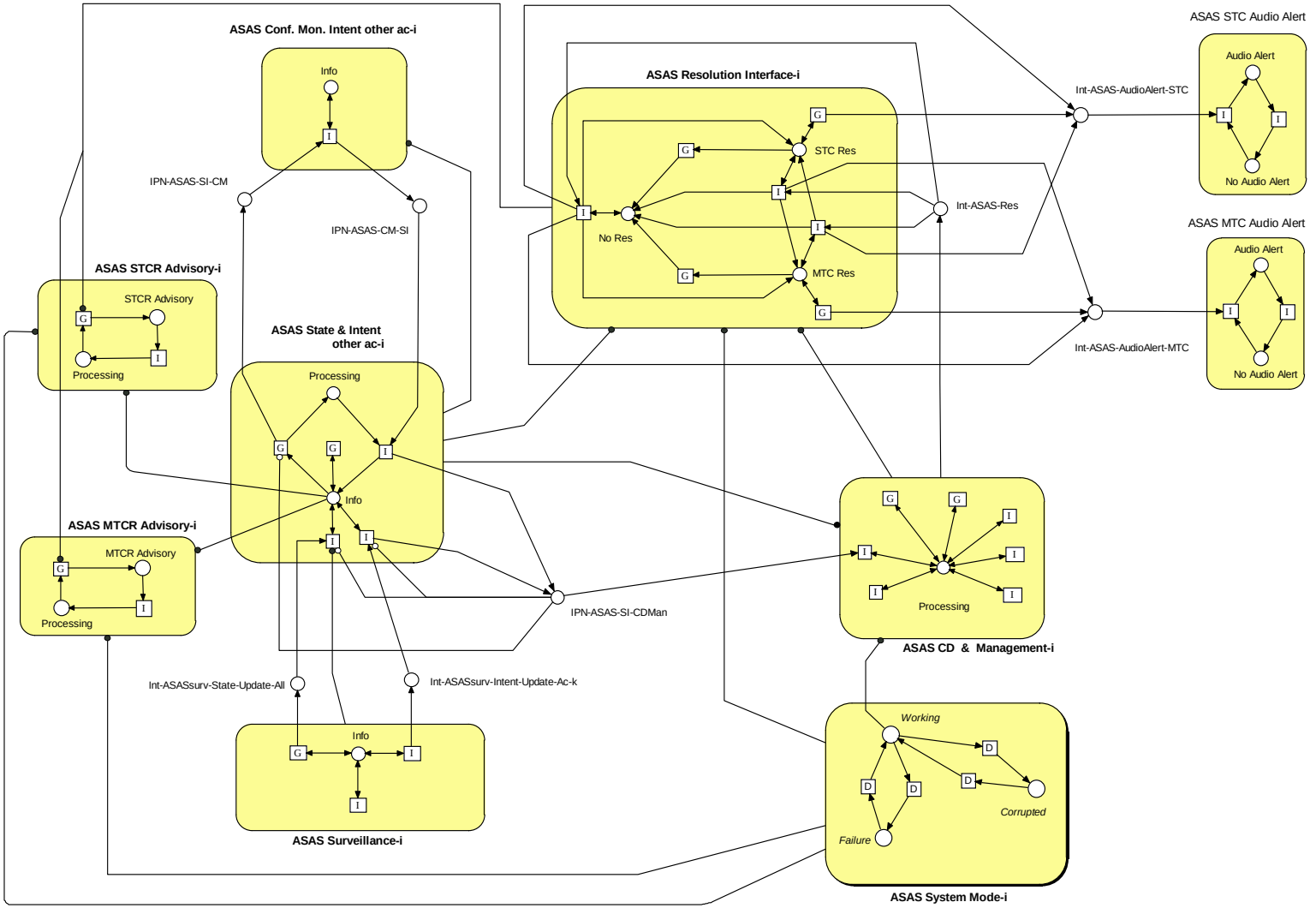

FIGURE 7: The agent ASAS in A^3 is modelled by ten LPNs, a number of ordinary and enabling arcs, and eight IPNs (with one place each).

The specific MTCR approach adopted works as follows:

- Each aircraft detects conflicts (5Nm/1000ft) 10 min. ahead.
- Aircraft nearest to destination has priority over other a/c.
- Aircraft with lowest priority has to make its 4D plan conflict free (15 min ahead) with all other plans.
- Undershooting of 5Nm/1000ft is allowed if there is no feasible conflict free plan and it does not create a short term conflict (this way everyone keeps on moving).
- Upon approval by the crew, the aircraft broadcasts the non-conflict-free 4D plan together with a message of being "Handicapped" (which is priority increasing).

Using the above approach, the MTCR part of ASAS computes an RBT advisory by a sequence of TCP's and turning angles. An MTCR Advisory applies to a medium term conflict, i.e. a conflict with any other aircraft within time horizon $[\tau_S, \tau_M]$. It is determined as the minimum turning angle (to the left or to the right) such that there are no predicted conflicts remaining with any aircraft which has higher priority than aircraft *i* and which is within horizon $[0, \tau_M + buffer_M]$. If there is no minimum turning angle possible below a certain value $\varphi_{M,\max}$, then the turning angle below $\varphi_{M,\max}$ is identified which provides the lowest underscoring of the minimum spacing criteria of 5Nm and 1000 ft between the RBT's. In that case aircraft *i* names itself handycapped. As soon as the advised MTCR advisories and the corresponding advisories have been implemented in the Airborne GNC agent of aircraft *i*, then these are broadcasted together with an handycap-i message. As remarked before, an MTCR Advisory is not allowed to create a short term conflict with any other aircraft.

The specific STCR approach adopted works as follows:

- Aircraft which detects conflict is obliged to resolve the conflict without awaiting any of the other aircraft
- Course change is identified using Velocity Obstacles (3 min. ahead)
- Conflict free means 3Nm/900ft minimal predicted miss distance
- Undershooting of these values is allowed if there is no feasible alternative (this way everyone keeps on moving)
- Upon approval by crew, the aircraft broadcasts its new course.

Using the above approach, the STCR part of ASAS computes a resolution course advisory. An STCR Advisory applies to conflicts with any other aircraft within time horizon of $[0, \tau_S]$. It is determined as the minimum turning angle (to the left or to the right) such that there are no predicted conflicts remaining with any aircraft and which is within the $[0, \tau_S + buffer_S]$ horizon. If there is no minimum turning angle possible below a certain value $\varphi_{S,\max}$, then the turning angle below $\varphi_{S,\max}$ is identified which provides the lowest underscoring of the minimum separation criteria.

Finally, there are two complementary LPN's:

- *LPN ASAS system mode* represents whether ASAS is working, failed, or corrupted (failed or corrupted mode also influences the ASAS resolution LPN's).
- *LPN ASAS Conformance Monitoring Intent of other a/c* compares for each other a/c *j* whether *j*'s state information agrees with *j*'s intent information. In case a significant difference is identified, then both Medium Term and Short Term CD&R of aircraft *i* is informed to stop using intent information of aircraft *j*.

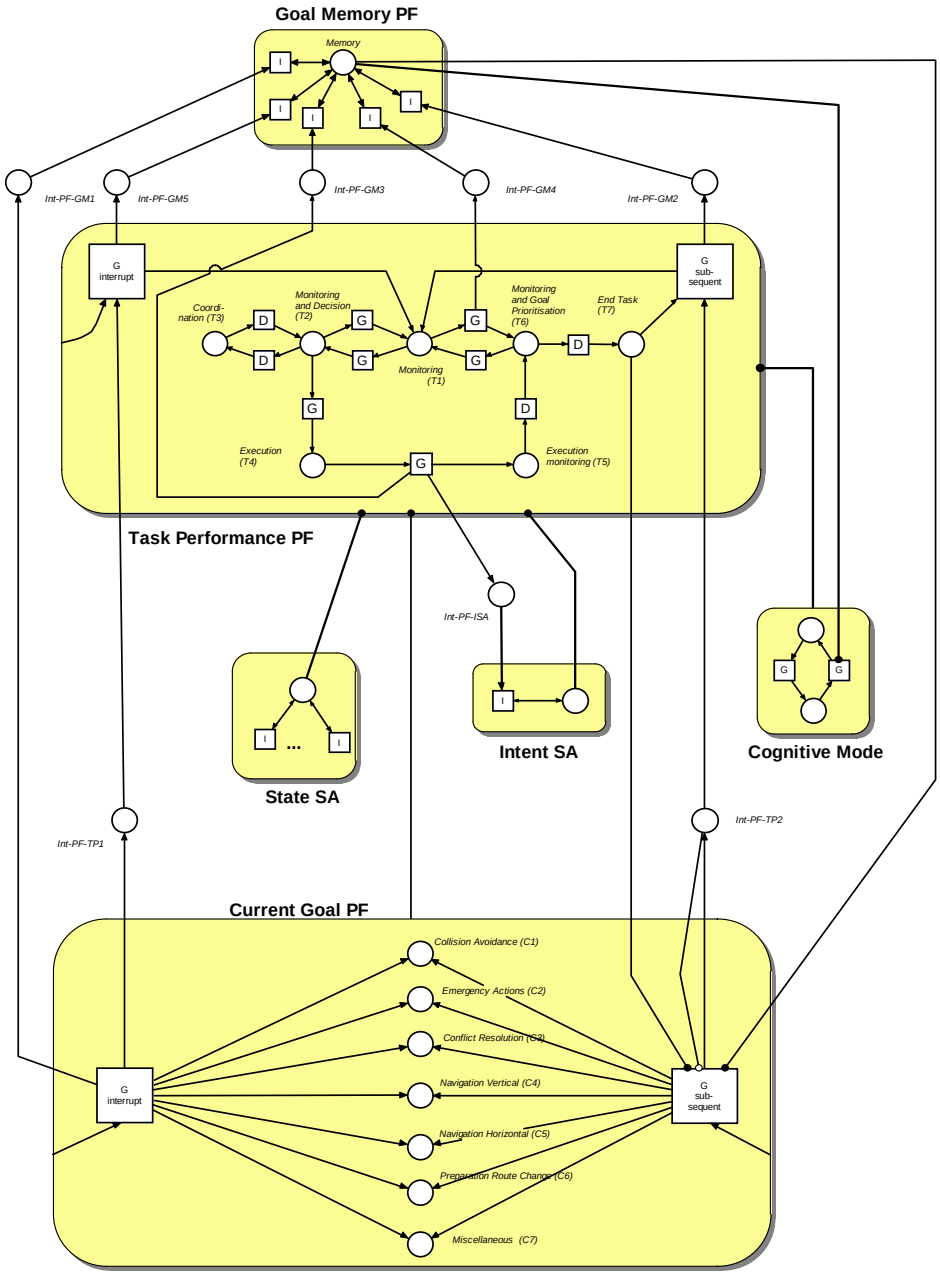

FIGURE 8: The agent Pilot-Flying in A^3 is modelled by six LPNs, and a number of ordinary and enabling arcs and some IPNs, consisting of one place and input and output arcs. The interconnections with other agents are not shown.

3.3 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 8.
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 interconnections with other agents are not shown in Figure 8. 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 8.
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.

3.4 Dimensions of Multi Agent Model

Now, we analyse the dimensions of the joint state space of the resulting Multi Agent Model. In Table 2 and Table 3, this is done for the agents ASAS and PF respectively, including all LPNs and all IPNs that end on one of these LPNs (i.e. incoming IPN's). The second column gives the number of places in the LPN or IPN. The third column gives the maximum state space of the colour used within an LPN or IPN. We also perform this analysis to the LPNs and IPNs of the other agents. The resulting number of product places and product state spaces is given in Table 4.

TABLE 2: Dimensional analysis of agent ASAS.

ASAS LPNs and IPNs	**Number of places**	**Maximum colour state space**
ASAS LPNs:		
Surveillance other aircraft	1	$\mathbb{R}^{N+1}$
State & Intent other aircraft	2	$\mathbb{R}^{20N+Nq+1}$
Conflict Detection & Management	1	$\mathbb{R}^{4N+10}$
Resolution Mode	3	$\mathbb{R}^{5N+5}$
STCR Advisory	2	$\mathbb{R}^{3q+6}$
MTCR Advisory	2	$\mathbb{R}^{3q+6}$
STC Audio alerting	2	$\varnothing$
MTC Audio alerting	2	$\varnothing$
Conformance Monitoring other aircraft	1	$\mathbb{R}^{15N}$
System Mode	3	$\varnothing$
ASAS internal IPNs:		
IPN-ASAS-SI-CM	1	$\mathbb{R}$
IPN-ASAS-CM-SI	1	$\mathbb{R}^2$

Int-ASAS-Res	1	$\varnothing$
Int-ASASsurv-State-Update-All	1	$\varnothing$
Int-ASASsurv-Intent-Update-Ac-k	N	$\varnothing$
IPN-ASAS-SI-CDMan	1	$\mathbb{R}$
Int-ASAS-AudioAlert-STC	1	$\varnothing$
Int-ASAS-AudioAlert-MTC	1	$\varnothing$
ASAS external IPNs:		
Int-FMS-ASASCD&Man	1	$\varnothing$
Int-NavVer-ASASCD	1	$\mathbb{R}^3$
Int-NavHor-ASASCD	1	$\varnothing$
Int-PNF-ASASCD&M	1	$\varnothing$
Int-GUID-STCR	1	$\mathbb{R}$
Int-GUID-MTCR	1	$\mathbb{R}$
Int-ASASsurv-Intent-Ac-k	N	$\varnothing$
Int-ASASsurv	1	$\varnothing$
Product	$288N^2$	$\mathbb{R}^{38+45N+(N+6)q}$

TABLE 3: Dimensional analysis of agent PF.

Pilot-Flying (PF) LPNs and IPNs	**Number of places**	**Maximum colour state space**
Pilot Flying (PF) LPNs:		
State Situation Awareness	1	$\mathbb{R}^7$
Intent Situation Awareness	1	$\mathbb{R}^5$
Goal memory	1	$\mathbb{R}^{19}$
Current goal	7	$\mathbb{R}$
Task performance	7	$\mathbb{R}^6$
Cognitive mode	2	$\mathbb{R}$
Pilot Flying (PF) internal IPNs:		
Int-PF-GM1	1	$\mathbb{R}^2$
Int-PF-GM2	1	$\mathbb{R}^2$
Int-PF-GM3	1	$\mathbb{R}$
Int-PF-GM4	1	$\mathbb{R}$
Int-PF-GM5	1	$\mathbb{R}^3$
Int-PF-TP1	1	$\mathbb{R}^4$
Int-PF-TP2	1	$\mathbb{R}^2$
Int-PF-ISA	1	$\mathbb{R}$
Pilot Flying (PF) external IPNs:		
Int-PF-Audio-PF	6	$\mathbb{R}^3$
Int-PF	1	$\varnothing$
Int-ASAS-ResCPU	1	$\varnothing$
Int-ASASCD-NavVer	1	$\mathbb{R}^{q+3}$
Int-FMSIntent-NavVer	1	$\varnothing$
Int-ASASCD-NavHor	1	$\mathbb{R}^{3q+5}$
Int-FMSIntent-NavHor	1	$\varnothing$
Int-PF-SSA-1	1	$\mathbb{R}$

Int-PF-SSA-2	1	$\mathbb{R}$
Int-PF-SSA-3	1	$\mathbb{R}$
Int-PF-SSA-4	1	$\mathbb{R}$
Int-PF-SSA-5	1	$\mathbb{R}$
Product	588	$\mathbb{R}^{71+4q}$

TABLE 4: Dimensional analysis of complete A^3 model.

Agent	**Number of product places**	**Maximum colour product state space**
Aircraft	4^N	$\varnothing$
Pilot Flying (PF)	588^N	$\mathbb{R}^{71N+4qN}$
Pilot-not-Flying (PNF)	8^N	$\mathbb{R}^{4N}$
AGNC	$(15\times 2^{15})^N$	$\mathbb{R}^{123N+9qN}$
ASAS	$(288N^2)^N$	$\mathbb{R}^{38N+45N^2+(N+6)Nq}$
Global CNS	16	0
Product	$\approx 16\times(2.7\times 10^{12}\times N^2)^N$	$\mathbb{R}^{(236+45N+Nq+19q)N}$

Table 4 brings into account that each type of agent, except global CNS, is applicable for each aircraft. The product places of the global CNS agent form the discrete-valued state space M^0. The corresponding continuous-valued state space is empty, which means that there is no dynamical behaviour connected to it. The product place of each other agent *i* forms the state space $M^i,\ i=1,..,N$.

Per aircraft, the number of product places is $\left|M^i\right| \approx 2.7\times 10^{12}\times N^2$. The colours attached to the places for each of the agents $i=1,\cdots,N$ form Euclidean-valued process components, assuming values in $\mathbb{R}^{236+45N+Nq+19q}$ with $\mathbb{R}^q$ representing the fixed dimension of an intent. If an intent consists of 5 TCP's (trajectory change points) and each TCP consists of a time and a 3D position then $q=4\times 5=20$, i.e. the dimension of this intent is $\mathbb{R}^{20}$. In Table 1 and Table 2 it is assumed that each intent has the same fixed dimension $\mathbb{R}^q$.

Each of the scenarios considered in the next subsection has eight aircraft, so $N = 8$.

This means that the number of product places equals $16\times(2.7\times 10^{12}\times 8\times 8)^8 \approx 1.3\times 10^{115}$, and that the product of the colour state spaces equals $\mathbb{R}^{9088}$ when $q=20$.

4 MC simulation model

4.1 From Petri net model to MC simulation model

Once the A^3 model has been specified in terms of Petri nets, the next phase consists of a systematic development of a corresponding Monte Carlo simulation model. This is done through the following sequence of steps:

- Identification of the scenarios that have to be evaluated through MC simulations, and identification of the safety relevant events that have to be counted during these MC simulations;
- Software coding. The SDCPN specification language of the Petri net model is transferred to any preferred computer coding language. For the A^3 model computer coding we used Borland's Delphi XE Professional coding language. Since SDCPN specification forms a detailed model, the transfer to Delphi code is rather straightforward;
- Software testing. This is done through conducting the following sequence of tests: random number generation, statistical distributions, common functions, each local Petri net implementation, each agent implementation, interactions between all agents, full MC simulation;
- Numerical approximation testing. This is needed to identify the maximum numerical integration step allowable, and the minimum number of particular MC simulations required for reaching statistically significant results;
- Development of suitable methods for the acceleration of the MC simulations for each of the identified scenarios, and implementation of these methods in the form of a software shell around the MC simulation model software;
- Graphical user interface testing. This is to verify that the input and output of data works well;
- Parameterization. The A^3 model has a set of 164 scalar parameters. The identification of parameter values is done through a search of literature, statistical sources, and complemented by conducting expert interviews. The fusion of complementary pieces of information is accomplished following a Bayesian approach.

4.2 Air traffic scenarios and safety related events

For the A^3 model, MC simulations are conducted for the following encounter scenarios:

- Two-aircraft head-on encounter scenario
- Eight-aircraft encounter scenario
- Random traffic scenarios for various traffic densities

The aim is to estimate for each scenario, probabilities for the following safety related events:

- Minimum Separation Infringement (MSI)
- Loss Of Separation (LOS) = $2/3^{rd}$ of MSI
- Near Mid Air Collision (NMAC)
- Mid Air Collision (MAC)

These safety related events are defined through two parameters: a horizontal distance criterion, and a vertical distance criterion. The specific values adopted for MSI, LOS, NMAC and MAC are given in Table 5.

TABLE 5. Definition of safety related events used in collecting statistics from the rare event MC simulations.

Event	MSI	LOS	NMAC	MAC
Horizontal distance (Nm)	3.0	2.0	1.0	0.054
Vertical distance (ft)	900	600	400	131

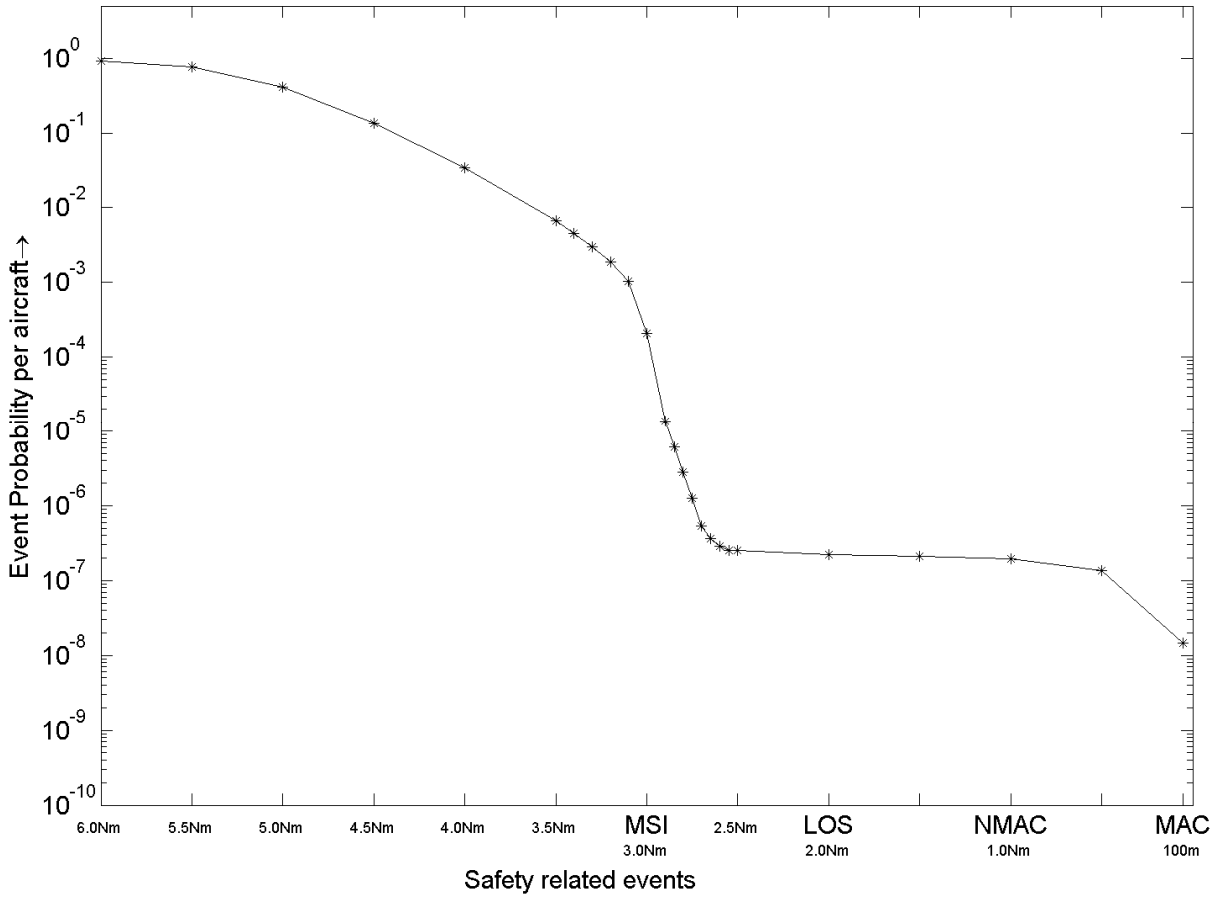

FIGURE 9. Illustration of the typical kind of results obtained through rare event simulation.

In addition to the MSI, LOS, NMAC and MAC events, the frequency of occurrence is measured for various intermediate distance values also. An illustrative picture of a possible resulting curve is provided in Figure 9. In this Figure, the horizontal axis is linear and typically runs from 6.0 Nm to 0.0 Nm miss distance (from left to right the miss distance reduces, which means that time runs from left to right also). The MAC point is only some 100 m away from the 0.0 Nm point. The vertical axis is logarithmic and covers 10 orders of magnitude in frequency of events (either per encounter or per flight hour).

For each encounter scenario simulation results are also given for the uncontrolled condition, i.e. in the A^3 model, the conflict detection and resolution is switched off. Under these uncontrolled condition, the safety related event probabilities in the various encounter scenarios have also been calculated using the gas model [Alexander, 1970; Endoh & Odoni, 1983]; these calculated values agreed with the estimated values obtained through MC simulation.

Because of the objective of the current report, the material in this report is focused on the results obtained for the A^3 ConOps. This is in contrast to [iFly D7.2g] where the focus is on the working of the rare event simulation methods. In [iFly D7.2g] the results for these different approaches are all shown. In this report the fused results are presented only.

4.3 Acceleration of MC simulation

The basic idea of assessing collision risk is to perform many Monte Carlo (MC) simulations with the A^3 model for each of the scenarios identified, and 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 MC simulation. This subsection describes the basic idea of how this works. As has been described in [iFly D7.1a], in case that straightforward MC simulation falls short in estimating safety risk, in such case we also exploit a sequential MC simulation approach, i.e. one which consists of a series of MC simulation cycles, where each cycle uses the output of the previous cycle as input to its own cycle. This way it is possible per cycle to zoom further into the behavior of A^3 model simulated trajectories. During the first simulation round we are interested in counting events that happen quite regularly, i.e. say once in about 10 to 100 MC simulation runs. Each next cycle we are interested in events that happen an order of magnitude less frequent. To make this cyclic approach work, the MC simulation results that have been obtained by one cycle are going to be used to partly generate the seeds for the next MC simulation cycle. In [Cerou et al., 2002, 2005] a precise mathematical framework and algorithm has been developed for conducting such a sequential MC simulation well. It also has been proven that the estimated event probabilities converge to the true probabilities under some technical conditions. The main conditions are that the process to be assessed needs to satisfy semi-martingale and strong Markov properties. The specific Petri net formalism that has been used for the A^3 model development and specification, assures that the technical conditions are satisfied [Krystul and Blom, 2005; Krystul, 2006; Krystul et al., 2007]. This general sequential MC simulation approach has been adapted towards the evaluation of the specific A^3 scenarios; this is described in [iFly D7.2g]. For advanced ATM,this IPS approach has been further developed [Blom, CDC2006, CDC2007, CRC2007, Wiley2009]

4.4 Model Parameter Values

Inherent to the early phase of A^3 ConOps development there are several parameters in the model for which it is not yet clear what the exact value should be. Therefore, one of the purposes in performing rare event simulation during this early ConOps development phase is to identify what the impact is of parameter values on the behaviour of the A^3 ConOps. Because there are 164 model parameters, it is not realistic to start such analysis for all 164 parameter values. Instead we work as follows:

Step 1: With the help of literature sources and various experts, for each model parameter a baseline parameter value has been identified; these baseline values are documented in Appendix B. For some key parameters in the A^3 ConOps model, baseline parameter values are given in Table 6 and Table 7. Table 6 provides the baseline minimum separation values proposed in [iFly D1.3] for the MTCR and the STCR of the A^3 ConOps. Table 7 provides the baseline dependability values adopted for the main safety critical parameters of the A^3 enabling technical systems (GNSS, ADS-B and ASAS). The baseline dependability values are based on [RTCA, 2002] and [Scholte, 2005].

TABLE 6. Baseline values of A³ ConOps model based MTCR and STCR parameters

	Look ahead time	**Horizontal separation**	**Vertical separation**	**Info used**	**Max turn angle $\varphi_{M,\max}$**
STCR	3 minutes + 10 sec	3Nm	900ft	State & Intent	$\varphi_{S,\max} = 60°$
MTCR	15 minutes	5Nm	1000ft	Intent	$\varphi_{M,\max} = 60°$

TABLE 7. Baseline values of key dependability parameters of A³ enabling technical systems

Math symbol	**Model parameters of A³ enabling technical systems**	**Baseline dependability**
p_{SAT}^{down}	Probability of GNSS down	1.0×10^{-5}
$p_{ADS,FRQ}^{occupied}$	Probability of Global ADS-B down[1]	1.0×10^{-6}
$p_{ADS,REC}^{down}$	Probability of Aircraft ADS-B Receiver down	5.0×10^{-5}
$p_{ADS,TRM}^{down}$	Probability of Aircraft ADS-B Transmitter down	5.0×10^{-5}
$p_{ASAS}^{corrupted}$	Probability of Aircraft ASAS performance corrupted	5.0×10^{-5}
p_{ASAS}^{fail}	Probability of Aircraft ASAS System down	5.0×10^{-5}

Step 2: The 164 model parameters have been walked through regarding their importance to assess the sensitivity of the assessed safety risk level to changes in their adopted value(s). This has led to the identification of the following six (groups of) parameters:

- Crew response delay parameters
- ASAS dependability parameters (See Table 7)
- Actual Navigation Performance (ANP) parameter
- MTCR horizontal separation parameter (See Table 6)
- STCR horizontal separation parameter (See Table 6)
- Groundspeed parameter

Step 3: Rare event simulations are repeated one-by-one for each of the six changes in the six (groups of) parameter(s) specified in Table 8.

Step 4: Evaluation of the simulation results obtained. In the current report the evaluation is directed to the meaning for the A³ ConOps.

TABLE 8. Parameter values identified for sensitivity analysis of A³ ConOps model

Id	**Parameter value scenario**	**Specific setting(s)**
0	Baseline	Baseline parameter values [iFLY D7.4, Appendix B]
1	Crew response delay	All crew response times in the model are reduced by a factor 2, i.e. the crew is expected to respond twice as fast as

[1] Global ADS-B down refers to frequency congestion/overload of data transfer technology used by ADS-B.

		has been assumed for the baseline.
2	ASAS dependability	10x and 100x better than the values in Table 5
3	ANP	ANP0.5 and ANP2 in contrast to baseline ANP1
4	MTCR	Horizontal separation 6Nm instead of 5Nm
5	STCR	Horizontal separation 5Nm instead of 3Nm
6	Groundspeed	300m/s instead of baseline 250m/s

4.5 Validation of A^3 model

Similar to the validation practices that have been well developed for computational aerodynamics [AIAA, 1998], overall validation consist of the following three complementary activities:

1) Qualification by domain experts of the activities modelled within each agent and interactions with other agents. Preferably these domain experts have not been involved with the A^3 model development;
2) Systematic comparison of MC simulation model outputs at the agent level with statistical data that have not been used for the A^3 model development; and
3) Systematic evaluation of the differences between model and reality and what effect these differences have in terms of bias and uncertainty in the assessed risk level [Everdij & Blom, 2002], [Everdij et al., PSAM2006].

For the A^3 model developed, the first validation activity has been performed by domain experts that were involved in the A^3 model development, but not yet by other domain experts. The second validation activity has not been performed, and remains for the following design and validation phase. This asks for collecting suitable statistical data that has not yet been used for the A^3 model development. In this report, the sensitivity analysis part of validation type 3 will be done for various key parameters. Completion of the bias and uncertainty analysis remains to done in follow-up design and validation phase.

On the basis of the verification and initial validation activities that have been conducted, we do not claim that the A^3 model is equal to a real A^3 operation. In the current study our A^3 model is primarily aimed at capturing well the interactions between the many types of agents in order to form an approximation of the true A^3 operation.

5 Two-aircraft encounters

5.1 Two-aircraft encounter scenarios

In these encounter scenarios, two aircraft start at the same flight level, some 320 km (173 Nm) away from each other, and fly on opposite direction flight plans head-on with a ground speed of approximately 250 m/s. The initial 3-dimensional position has standard deviations of 20m along the RBT centerline, 0.5Nm in the lateral direction (RNP1) and 20m in height.
The parameter value scenarios considered are those specified in Table 8. For each parameter setting both a standard MC and a Hierarchical Hybrid IPS (HHIPS) has been conducted. For the assessment of each scenario for one set of parameter values, we ran both a standard MC simulation and 10 times an HHIPS based Sequential MC (SMC) simulation [Blom CDC2007, Wiley2009]. Table 9 shows the number of MC runs or the number of particles used, and the time-duration of the simulation.

TABLE 9. Parameter value scenarios simulated, MC types and time durations of the computations on two Dell precision T7500.

Id	Parameter value scenario	Figure	Standard MC		HHIPS based SMC	
			# of runs	Duration	# of particles	Duration
0	Baseline	10	28 million	12 hrs	10×80 thousand	1 hr
1	Crew response	11	4 million	2 hrs	10×80 thousand	1 hr
2	Dependability	12	4 million	2 hrs	10×80 thousand	1 hr
3	ANP	13	0.7 million	<1 hr	10×80 thousand	1 hr
4	MTCR	14	1.5 million	<1 hr	10×80 thousand	1 hr
5	STCR	15	0.8 million	<1 hr	10×80 thousand	1 hr
6	Groundspeed	16	1.5 million	<1 hr	10×80 thousand	1 hr

The total duration of using both Dell machines for the running of simulations for two aircraft encounter scenarios amounts 24 hours, which comes down to running the two Dell computers 1 day full time. In practice, there also is an order in magnitude more days needed for the preparation of the simulations (including testing of the software adaptations), and for the evaluation and documentation of the results obtained. Comparison of the standard MC and HHIPS simulation results are presented and discussed in [iFly D7.2g]. In this section we focus on what the combined result means for the A^3 ConOps.

5.2 Simulation results

The simulation results for parameter value scenarios 0 through 6 are shown in Figures 10 through 16. The curves are obtained by fusion of the results obtained through running standard MC simulations and HHIPS. In this subsection we only address the meaning of these results for the A^3 ConOps.
Figure 10 presents the estimated probabilities for the baseline parameter values. Figure 10 also provides the MC simulation results for the uncontrolled case. Then the estimated probabilities of NMAC and MAC are 0.9 and 0.07 respectively. Thus for the two-aircraft scenario considered, without A^3 control and without ACAS, there is a 90% chance that an

NMAC happens and subsequently there is 7% chance that a MAC happens.

The A^3 controlled results in Figure 10 show that in the A^3 model, conflict detection and resolution works quite effectively in avoiding MSI; only about one in 5000 (= 1.0 / 2.0E-4) head-on encounters leads to an MSI. Moreover, under baseline dependability, about one in 800 (= 2.0E-4 / 2.5E-7) of such MSI's leads to a LOS. This means that the A^3 model is very effective in preventing LOS for a head-on encounter between two aircraft. The results also show that A^3 performs its work before reaching LOS. This means that A^3 seems to avoid competition with ACAS, although formally this remains to be verified by including ACAS model in the MC simulation.

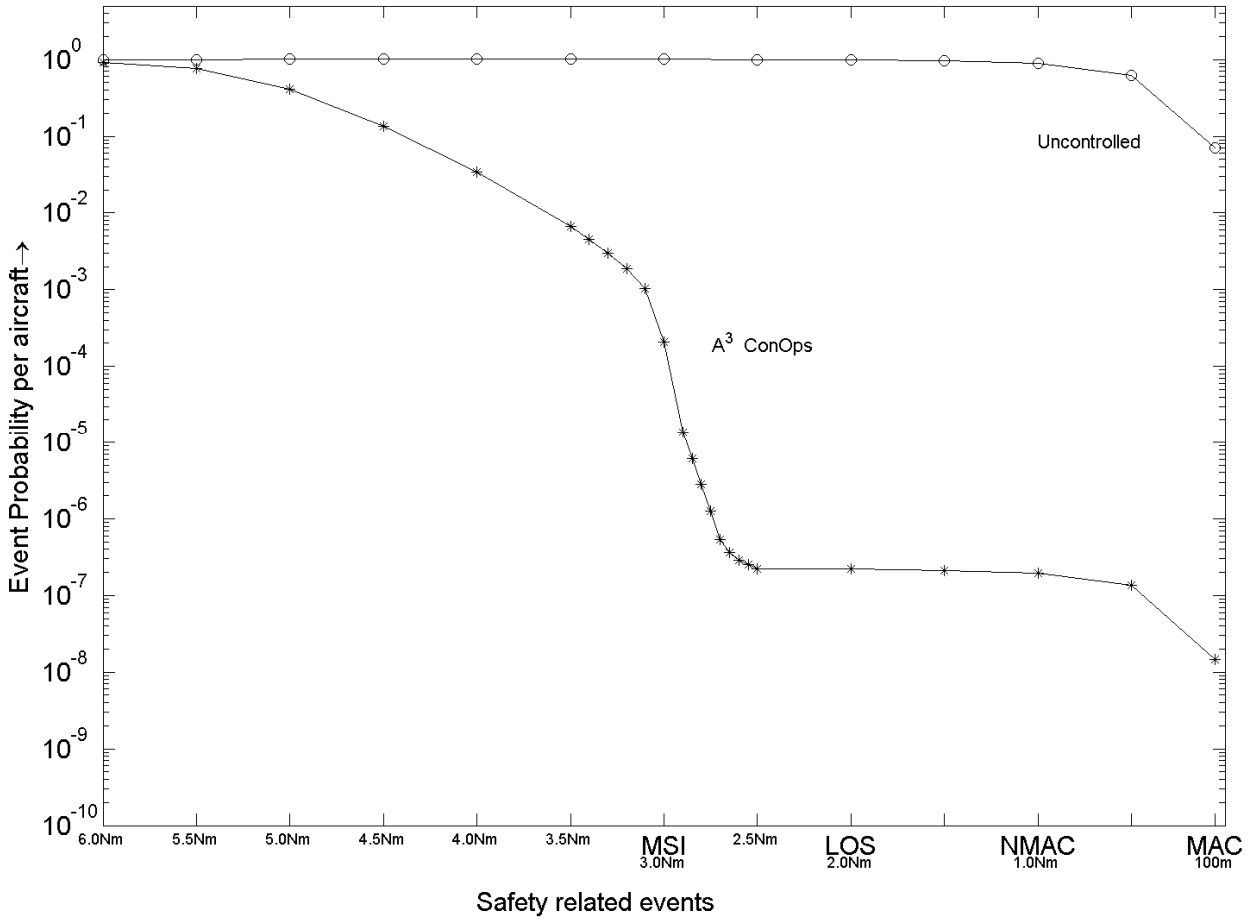

FIGURE 10: Estimated event probability for two-aircraft head-on encounter uncontrolled (○) *and under A^3 model (*) with baseline parameter values.*

By comparing, in Figure 10, the right halves of the curve for the A^3 ConOps against the uncontrolled curve, it can be seen that there these two curves are a fixed factor away from each other. This factor amounts $\frac{1}{4}$x10^{-6} for the baseline dependability values.

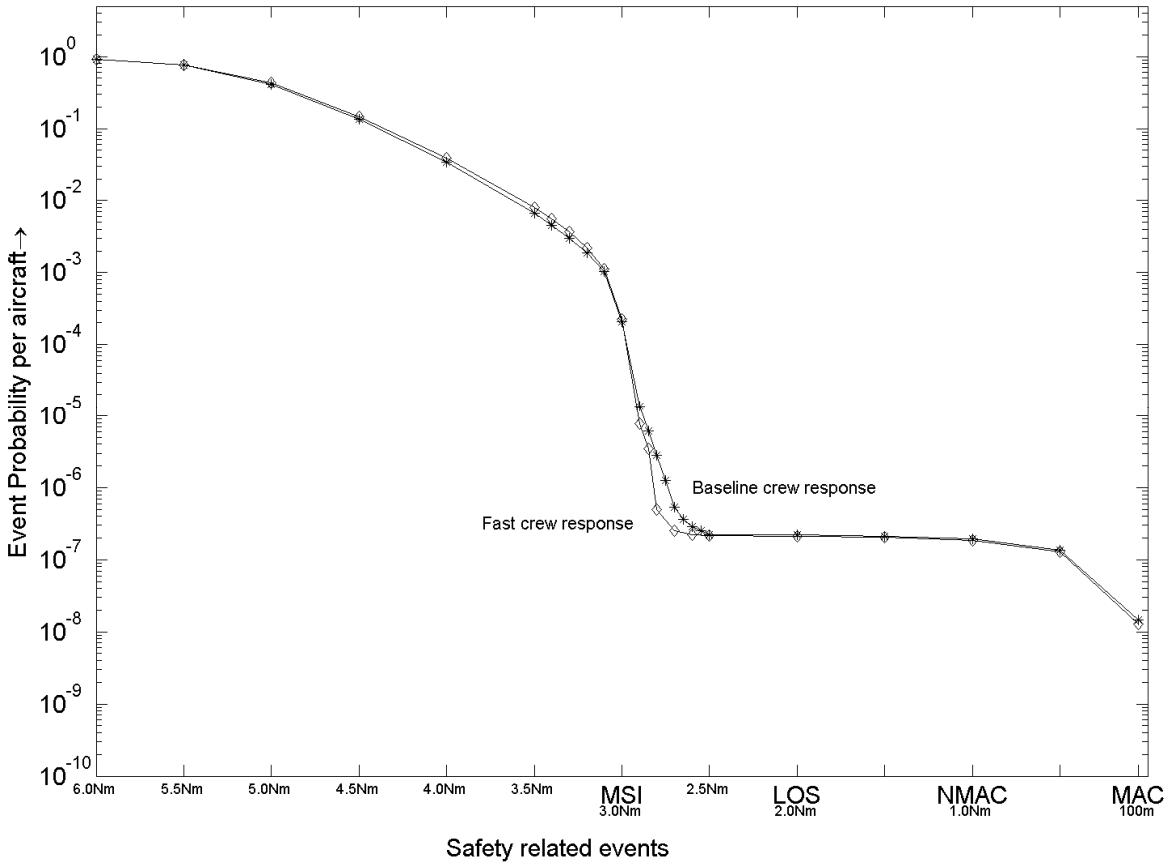

*FIGURE 11: Effect on rare event probabilities of varying crew response values. * = Baseline crew response parameter values, ◊ = Fast crew response parameter values.*

The curves in Figure 11 show that the sensitivity to crew response does not play a key factor.

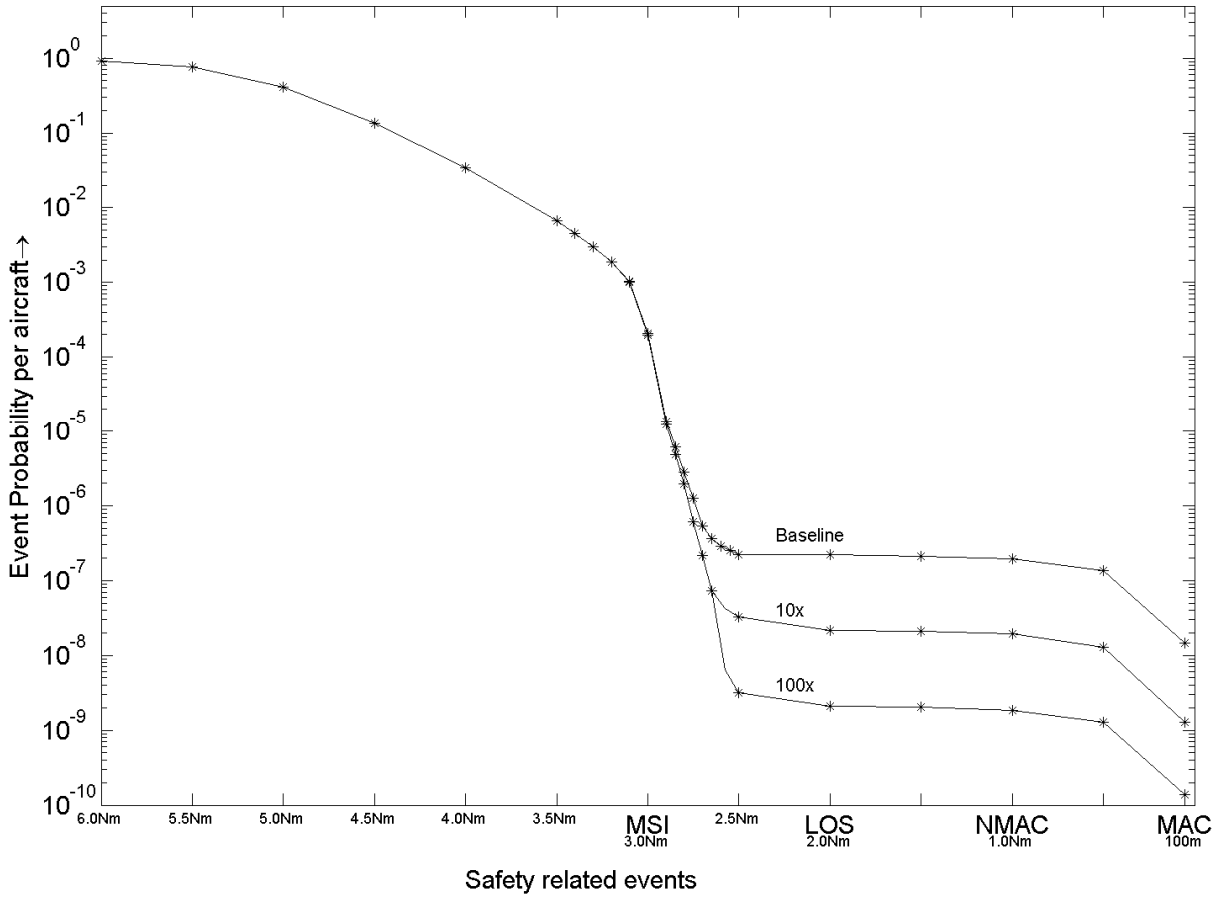

FIGURE 12: Effect on rare event probabilities of improving ASAS dependability by factors 10x and 100x respectively.

Figure 12 presents estimated probabilities for the safety related events defined in Table 8 under A^3 control for three sets of dependability parameter values. The results in Figure 12 clearly show that for the two aircraft head-on encounter, the 10- and 100-fold improvements in the dependability of A^3 enabling technical systems lead to 10- and 100-fold improvements respectively in the estimated LOS, NMAC and MAC probabilities, whereas the estimated MSI probabilities remain unchanged. This is in line with the finding that the cause for collision risk in this scenario lies in the dependability of A^3 enabling technical systems. Moreover, the results show that for a two aircraft encounter the A^3 model reduces the probabilities for LOS, NMAC and MAC by improving the dependability of the A^3 enabling technical systems.

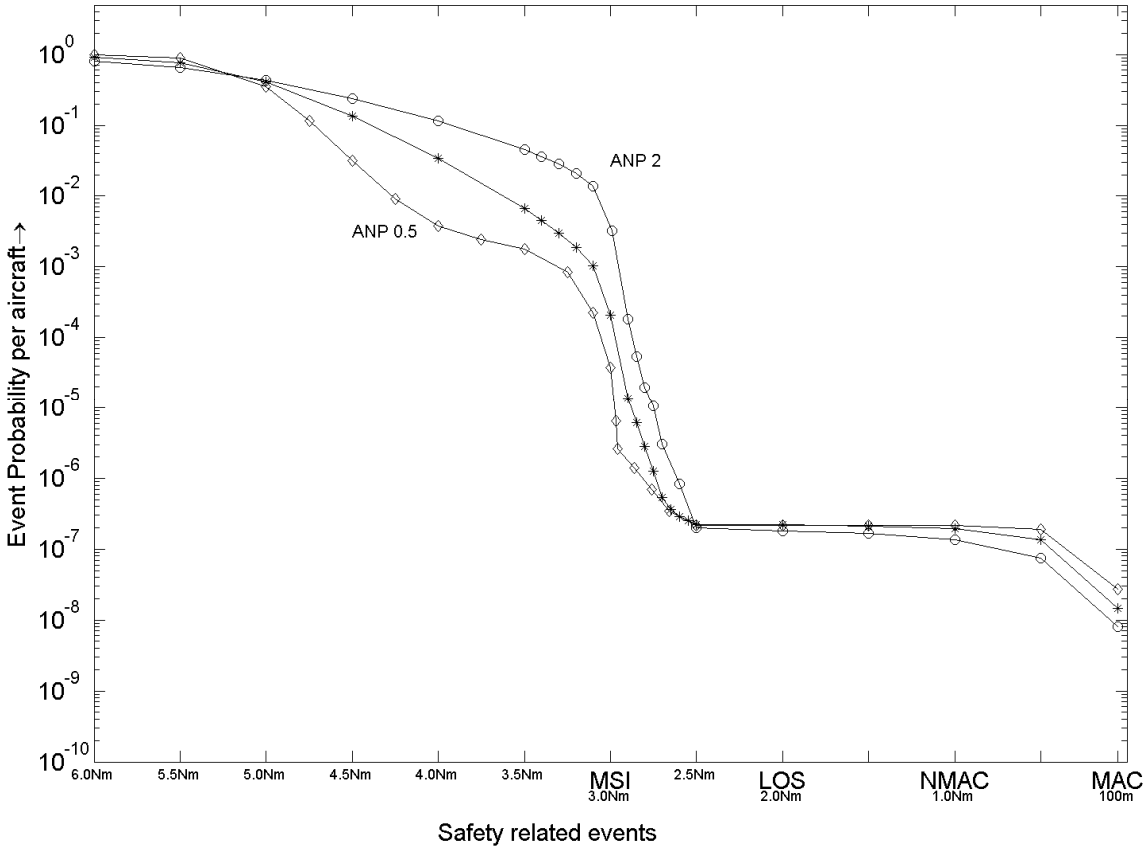

*FIGURE 13: Effect on rare event probabilities of varying ANP values. * = ANP1 (baseline), ○ = ANP2, ◊ = ANP0.5.*

Figure 13 shows that a change in ANP value has a significant impact on the curves for events happening prior to MSI. Figure 13 also shows that the sharp reduction that starts to work around MSI, keeps on working well. Hence from a safety risk perspective the ANP value does not have a large impact. In fact the largest effect then appears at MAC value; the larger the ANP value is, the lower the MAC frequency is.

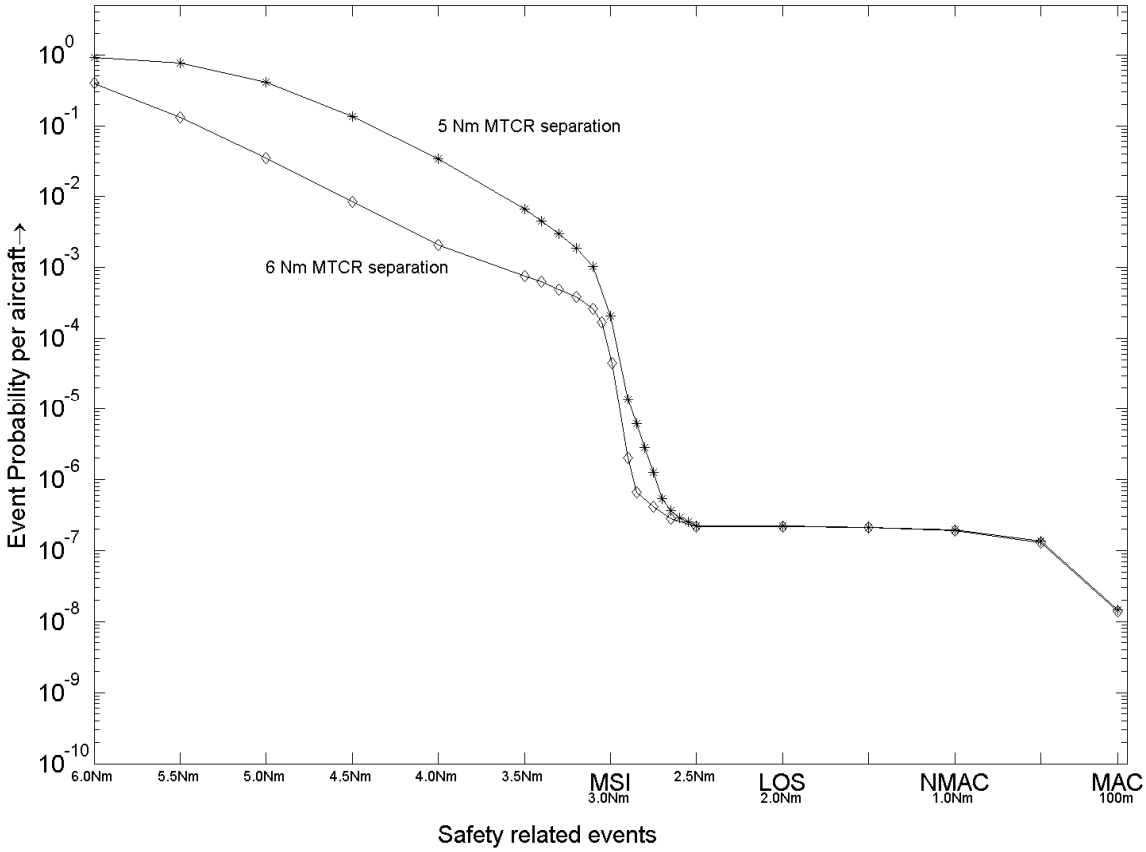

*FIGURE 14: Effect on rare event probabilities of varying MTCR separation values. * = 5 Nm (baseline), ◊ = 6 Nm.*

Figure 14 shows that an increase of MTCR separation value from 5 Nm to 6 Nm has a significant impact on the curves for values above MSI. Figure 14 also shows that the sharp reduction that starts to work around MSI keeps on working well. Hence from a safety risk perspective the MTCR value does not have a large impact.

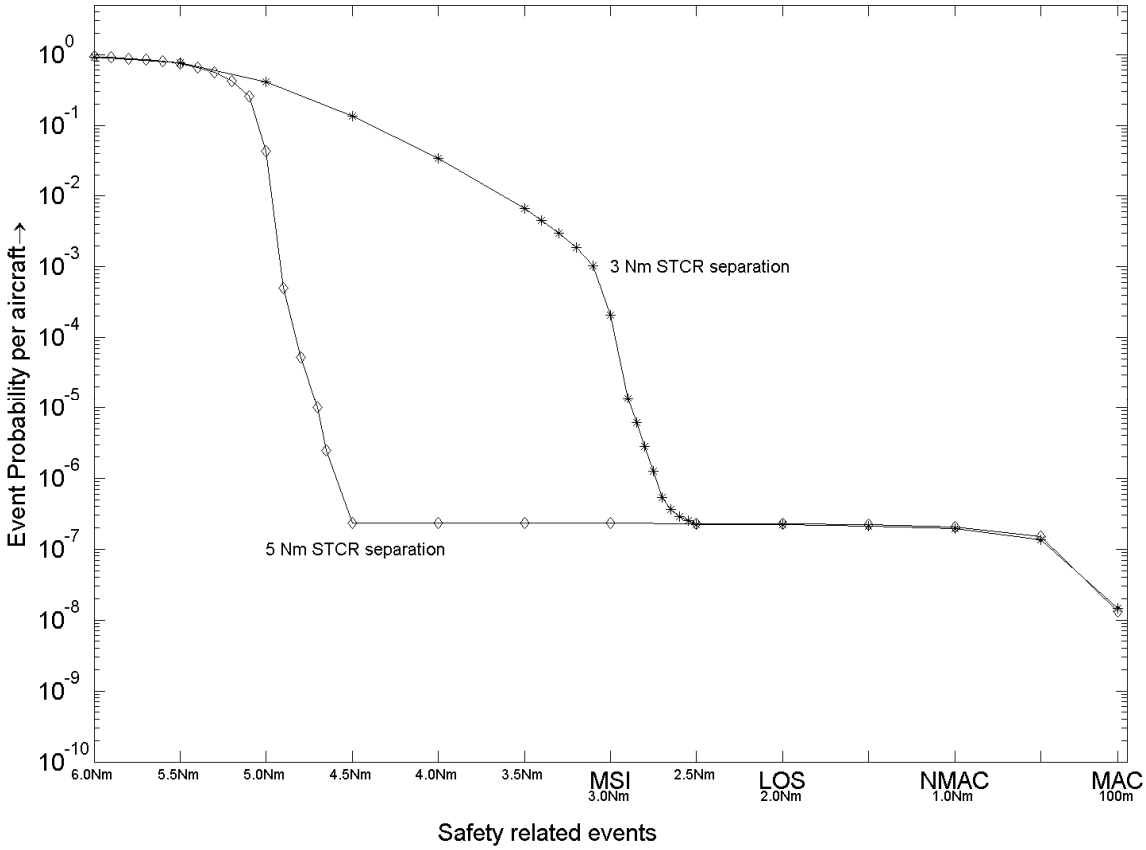

*FIGURE 15: Effect on rare event probabilities of varying STCR separation values. * = 3 Nm (baseline), ◊ = 5 Nm.*

Figure 15 shows that an increase of STCR separation value from 3 Nm to 5 Nm has a large impact on the curves. Figure 14 shows that the sharp reduction that worked around 3 Nm is now already working around 5 Nm.

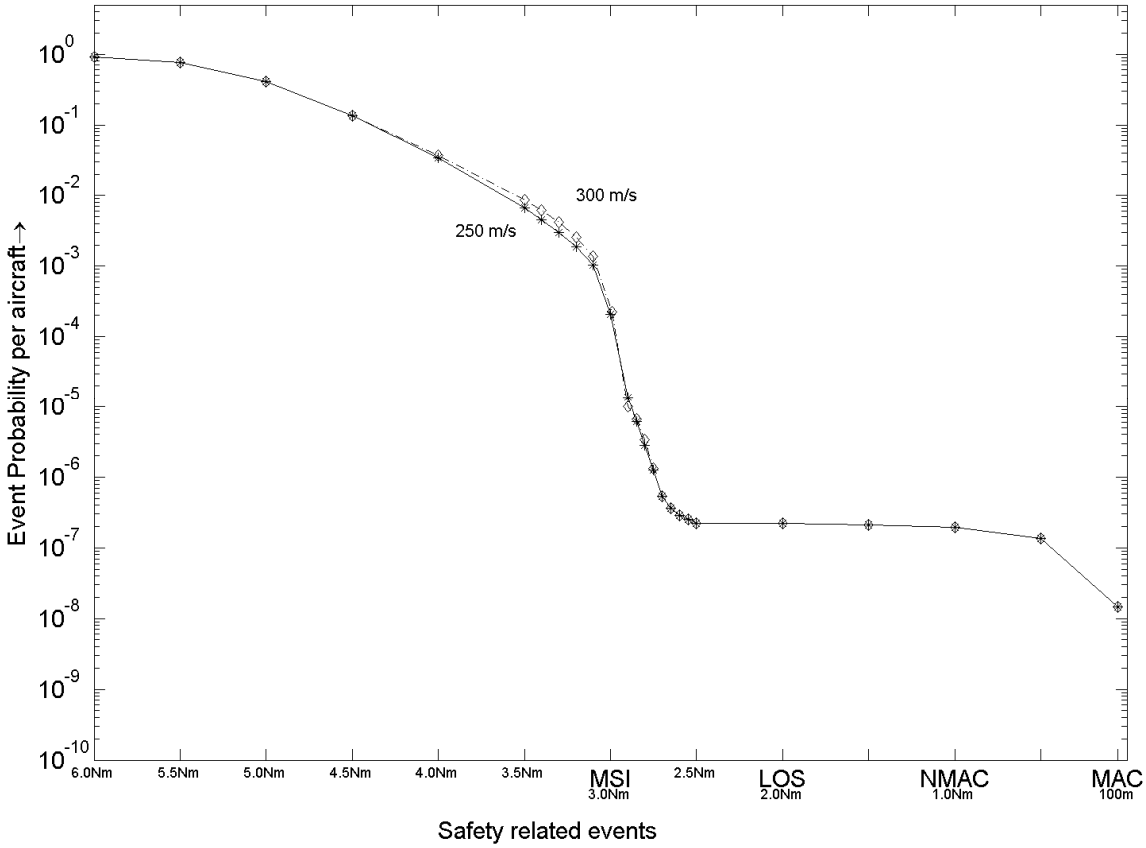

*FIGURE 16: Effect on rare event probabilities of varying Groundspeed. * = 250 m/s (baseline), ◊ = 300 m/s.*

The curves in Figure 16 show that the sensitivity to groundspeed does not play a key factor.

6 Eight-aircraft encounter

6.1 Eight-aircraft encounter scenarios

Next we consider the eight-aircraft encounter scenario pictured in Figure 17. Each aircraft starts at the same flight level and from a circle of about 320km (173 Nm) in diameter. The initial 3-dimensional position has standard deviations of 20m along the RBT centerline, 0.5Nm in the lateral direction (RNP1) and 20m in the height. Each aircraft has a ground speed of 250 m/s and is heading to the opposite point on the circle.

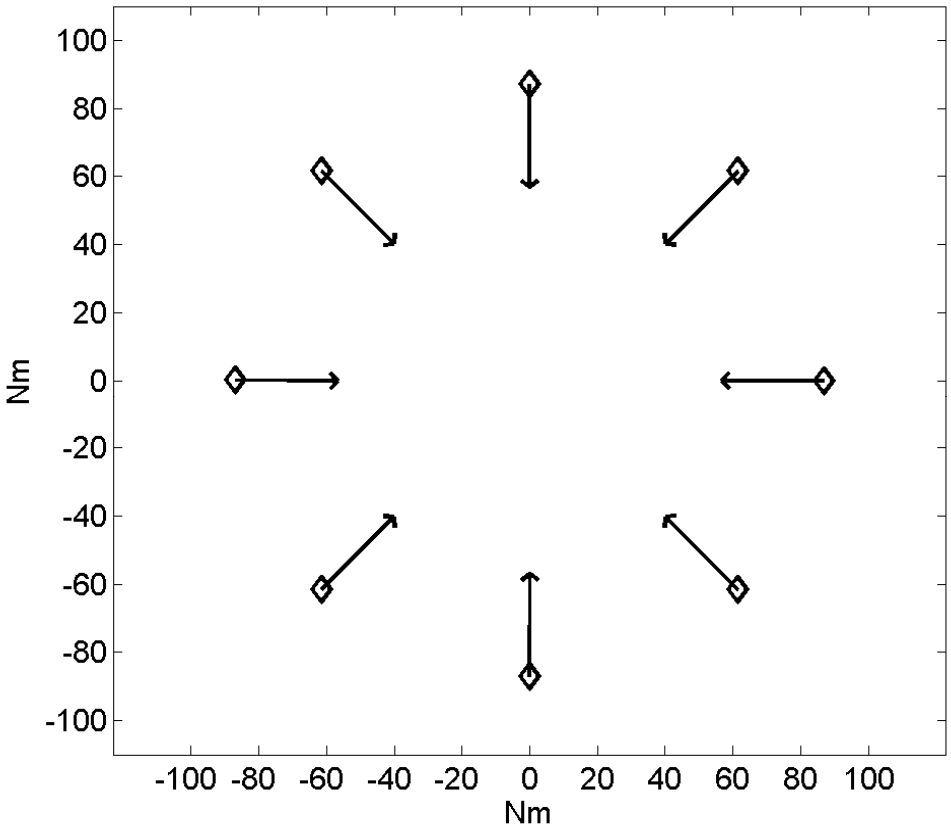

FIGURE 17: Eight aircraft encounter scenario at same flight level

Because of random initial conditions and random disturbances, each MC simulated eight aircraft encounter generates trajectories that differ from those generated before. Figure 18 shows a top view of an example of trajectories that are generated for the eight-aircraft encounter scenario under the A^3 concept of operation.

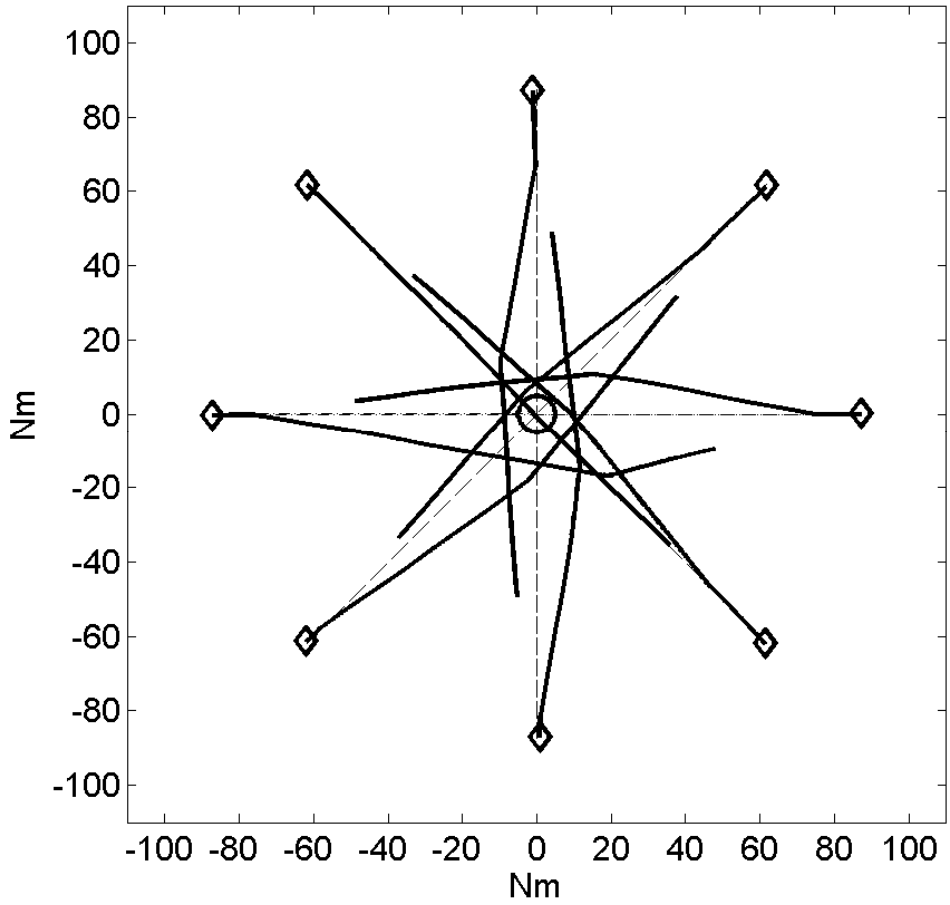

FIGURE 18: A[3] *generated conflict resolutions example for eight aircraft encounter scenario; ◊ = start of simulated trajectory. The circle in the centre has a 10 Nm diameter.*

The parameter value scenarios considered are those specified in Table 8. For each parameter setting a standard MC is conducted. For the baseline scenario also an IPS based SMC [Blom, CDC2007; CRC2007] is conducted. The number of MC runs or the number of particles used is given in Table 10. In addition, Table 10 shows the time-duration of the simulation. Because the standard MC simulation is so time demanding, for the baseline scenarios only a large number of MC runs has been simulated.

TABLE 10. Parameter value scenarios simulated, MC types and time durations of the computations on two Dell precision T7500

Id	Parameter value scenario	Figure	Standard MC		IPS based SMC	
			# of runs	Duration	# of particles	Duration
0	Baseline	19	14 million	207 hours	12× 15 thousand	7.5 hours
1	Crew response	20	1.2 million	19 hours	-	-
2	Dependability	21 *)	-	-	-	-
3	ANP	22	0.6 million	10 hours	-	-
4	MTCR	23	0.64 million	11 hours	-	-
5	STCR	24	1.2 million	19 hours	-	-
6	Groundspeed	25	0.72 million	12 hours	-	-

*) Figure 21 is obtained by performing a systematic analysis of the standard MC simulation results obtained for the baseline scenario.

The total duration of using both Dell machines for the running of simulations for eight aircraft encounter scenarios amounts 285 hours, which comes down to running the two Dell computers 12 days full time. In practice, there also are a similar number of days needed for the preparation of the simulations (including testing of software adaptations), and for the evaluation and documentation of the simulation results obtained. Comparison of the standard MC and IPS based simulation results are presented and discussed in [iFly D7.2g]. In this section we focus on what the combined result means for the A^3 ConOps.

6.2 Simulation results

The simulation results are shown in Figures 19 through 25. In this subsection we address the meaning of this for the behavior of the A^3 model.

Figure 19a presents the event probability results for the eight aircraft encounter scenario, uncontrolled and under A^3 control at baseline parameter values. Without control, the estimated probability of MSI, NMAC and LOS for an individual aircraft are all equal to 1.0 while for MAC the probability is approximately 0.33.
In Figure 19b, the event probabilities under A^3 control for the eight-aircraft encounter scenario are compared to the probabilities obtained for two-aircraft head-on encounter scenario, both under baseline parameter values.

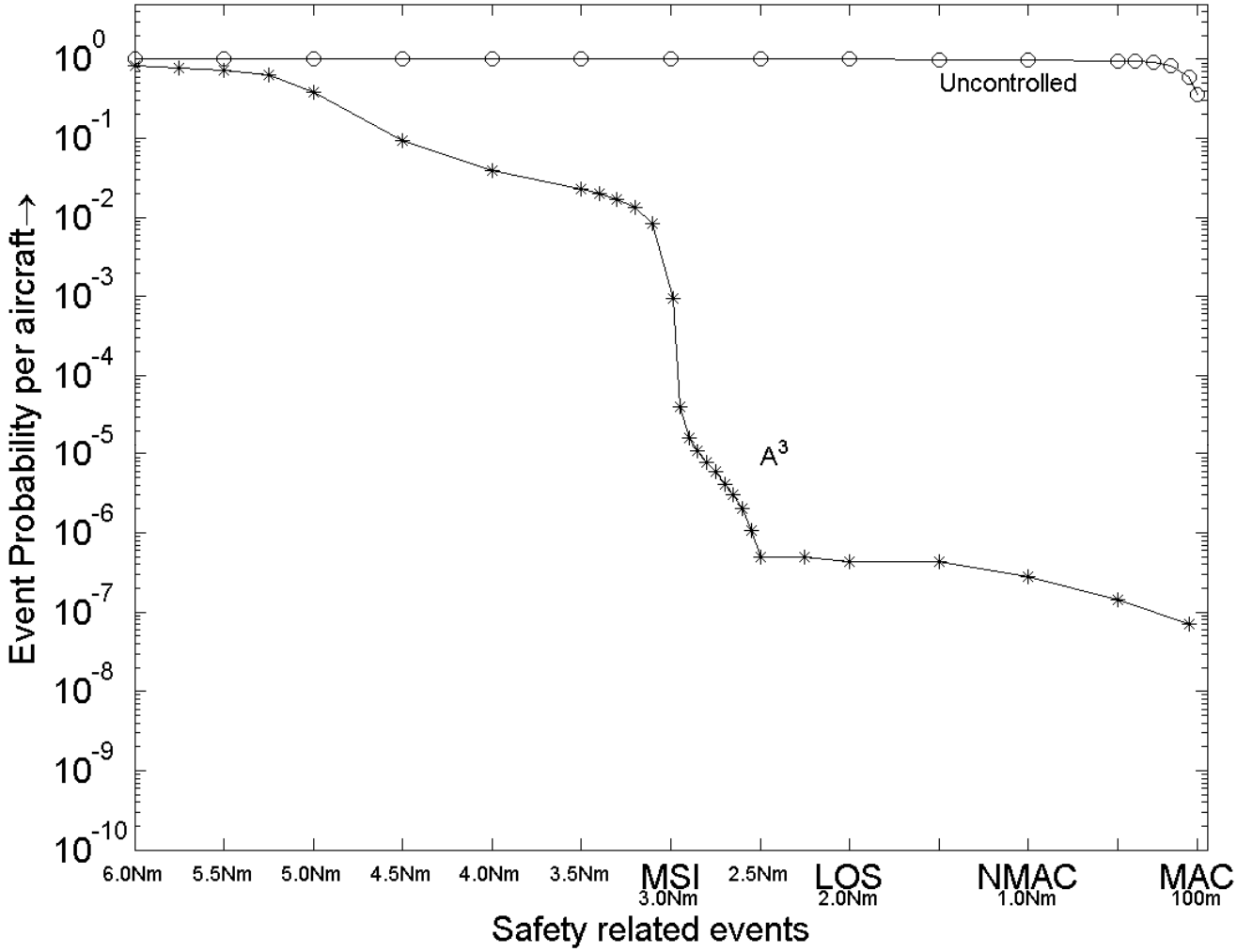

FIGURE 19a. Estimated probabilities of safety related events per aircraft for eight-aircraft encounter uncontrolled (○) *and under* A^3 *model (*) with baseline parameter values.*

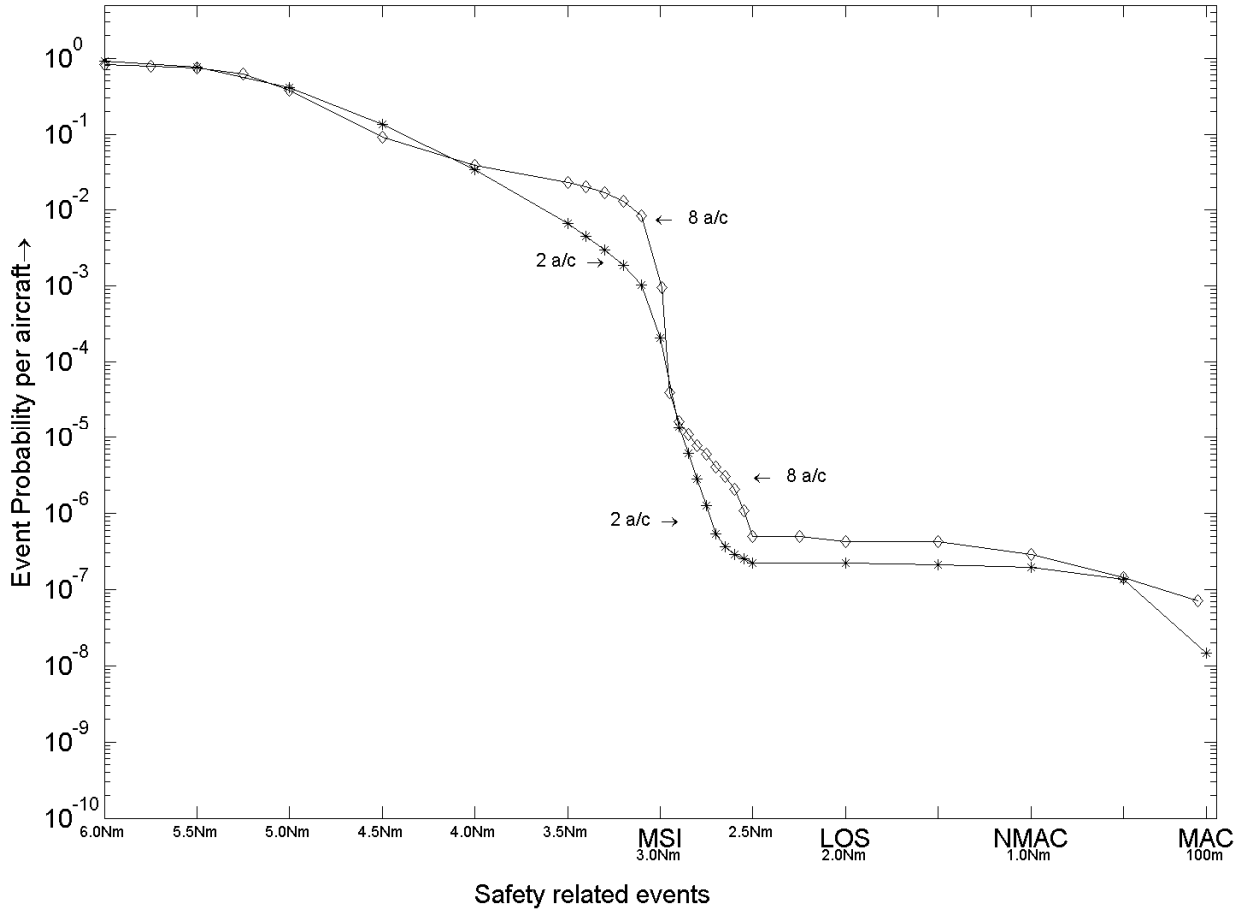

FIGURE 19b. Estimated probabilities of safety related events per aircraft in two-aircraft head-on encounter(*) vs. eight-aircraft encounter (◊)

Figure 19b shows that the MSI probability for the eight-aircraft encounter is a factor 5 (= 1.0E-3 / 2.0E-4) times higher than for the two-aircraft encounter, while there are 7 times more aircraft to collide with. From an MSI probability perspective, the results obtained for the eight-aircraft encounter show that A^3 is performing remarkably well. The LOS and NMAC probabilities for the eight-aircraft encounter are of the same magnitude as for the two-aircraft encounter. Thus also for these rare events A^3 is doing very well.

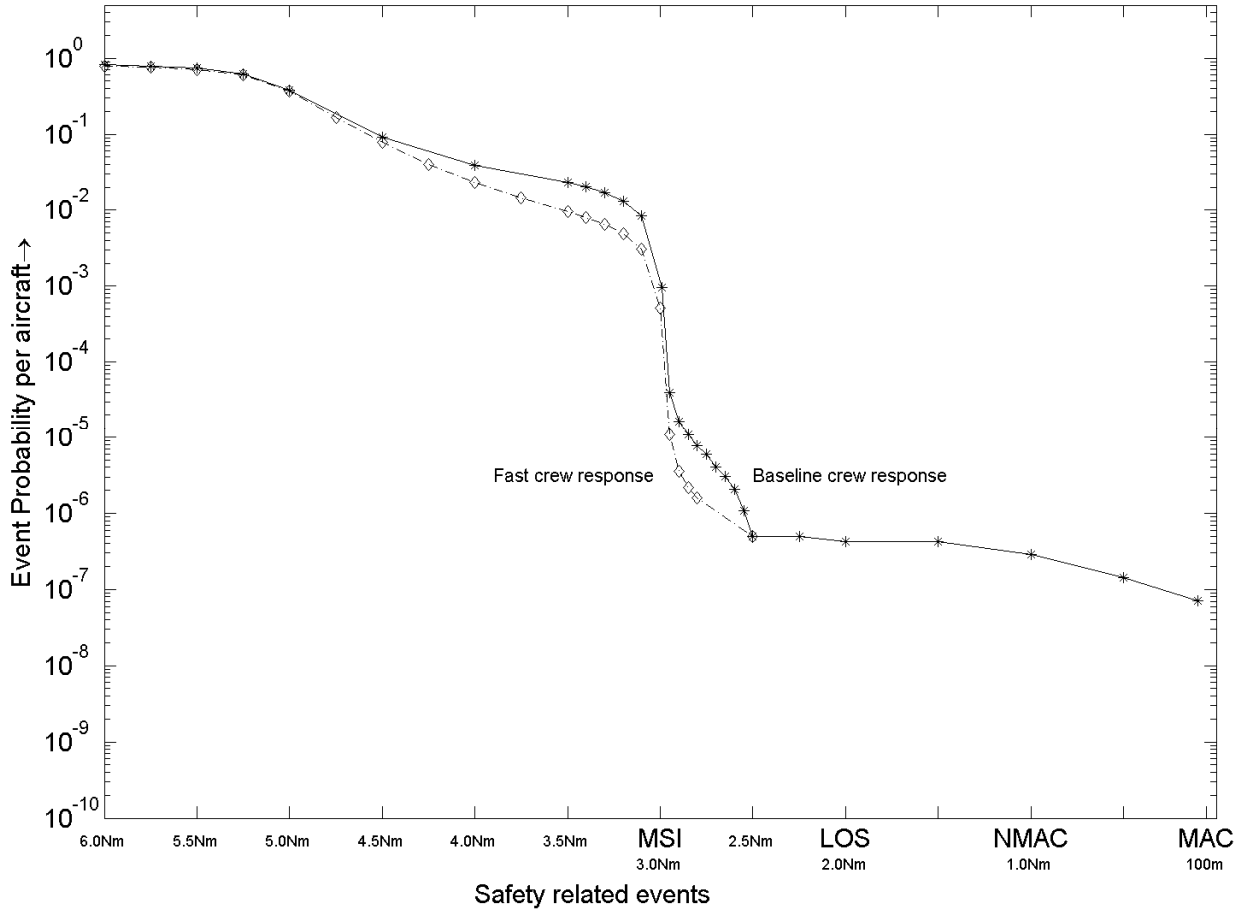

*FIGURE 20: Effect on event probabilities of crew response values. * = Baseline crew response parameter values, ◊ = Fast crew response parameter values.*

Figure 20 shows the sensitivity of the A^3 results for crew response. When crew response values are a factor two lower than baseline values the footing in the curve for values between 3 and 2.5 Nm disappears. This means that for the eight aircraft encounter scenario, crew response is a factor that should not be ignored.

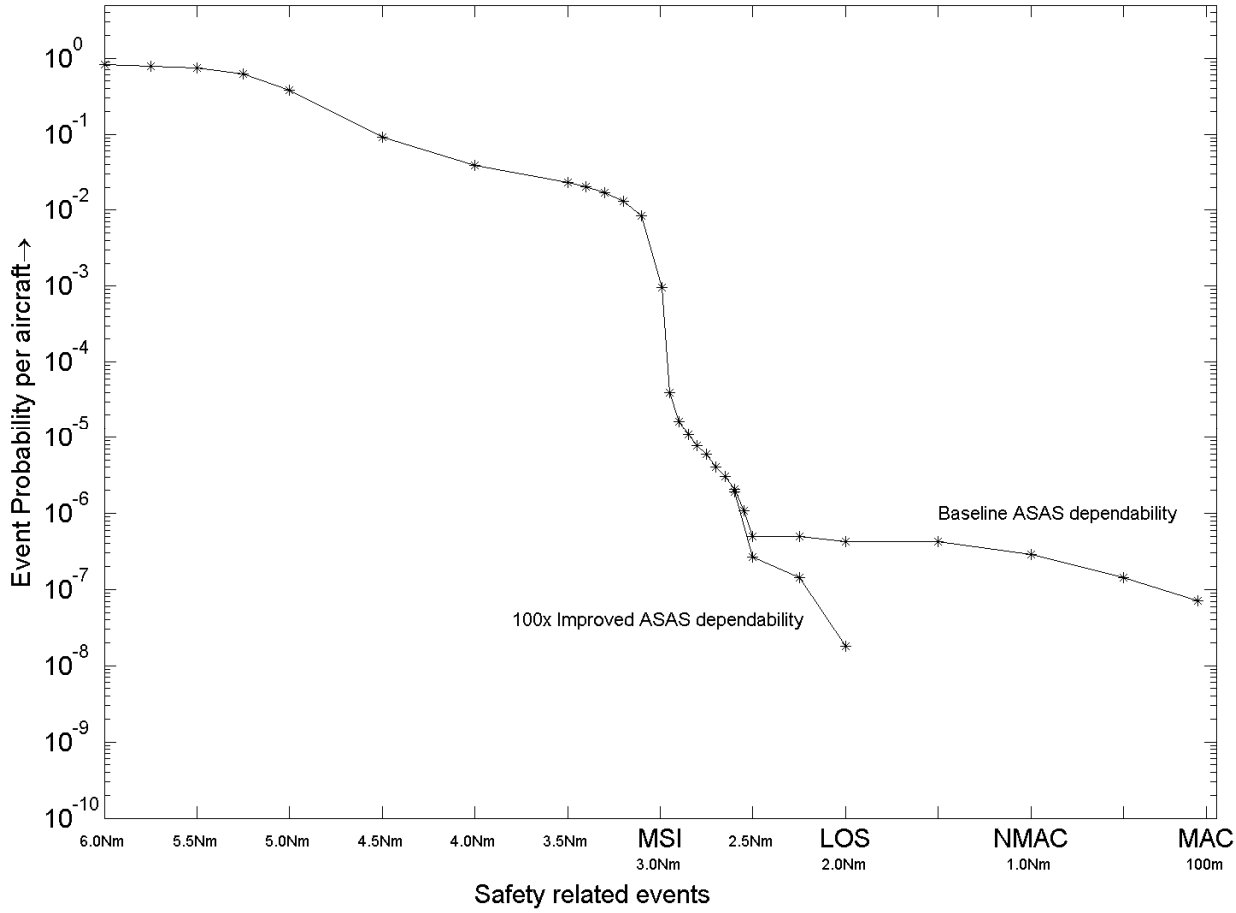

FIGURE 21a: Effect on event probabilities of improving the dependability values for GNSS, ADS-B and ASAS systems by a factor 100x.

Figures 21a-b show the effect of improving the dependability of ASAS technical support systems by a factor 100. The results in Figure 21a demonstrate a healthy improvement of the rare event frequencies in case the dependability value of ASAS technical support systems is improved by a factor 100.

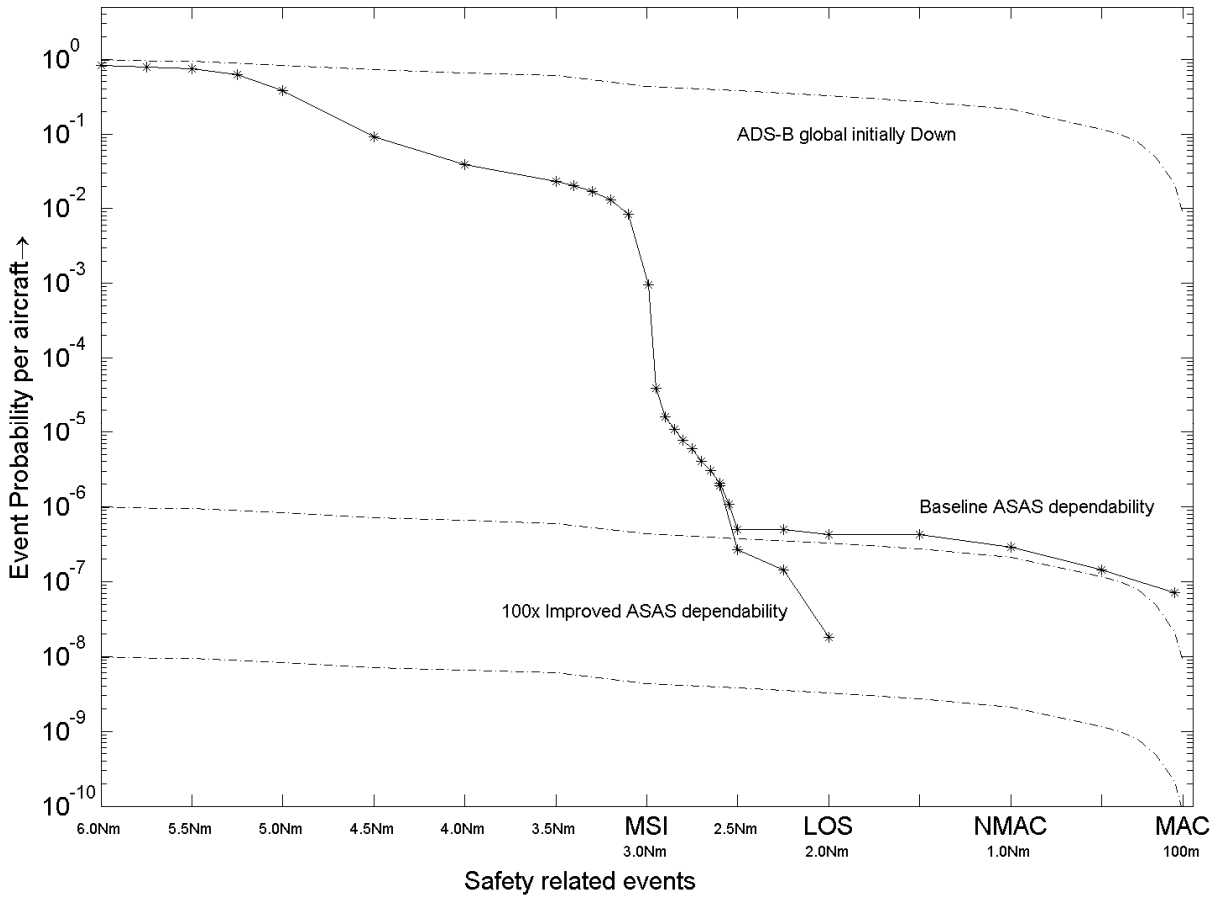

FIGURE 21b: The additional dashed curve at the top of the Figure is obtained by running standard MC simulations for the case that ADS-B is initially Down. The other two dashed curves are constructed by copying the top level curve at a lower level by a factor 10^{-6} *and a factor* 10^{-8} *respectively.*

Because the MC simulation results for a 100x improved dependability of ASAS related systems did not deliver (reliable) probability values for LOS, NMAC and MAC, in Figure 21b some extra curves have been inserted to show the expected behavior of A^3 ConOps for LOS, NMAC and MAC values. First the curve at the top has been obtained by running standard MC simulations with the A^3 ConOps model under the initial condition that ADS-B global is Down. Next this curve has been copied at factors 10^{-6} and 10^{-8} down respectively. These factors represent baseline and 100x better values for the probability values adopted for Global ADS-B being down (second item in Table 7).

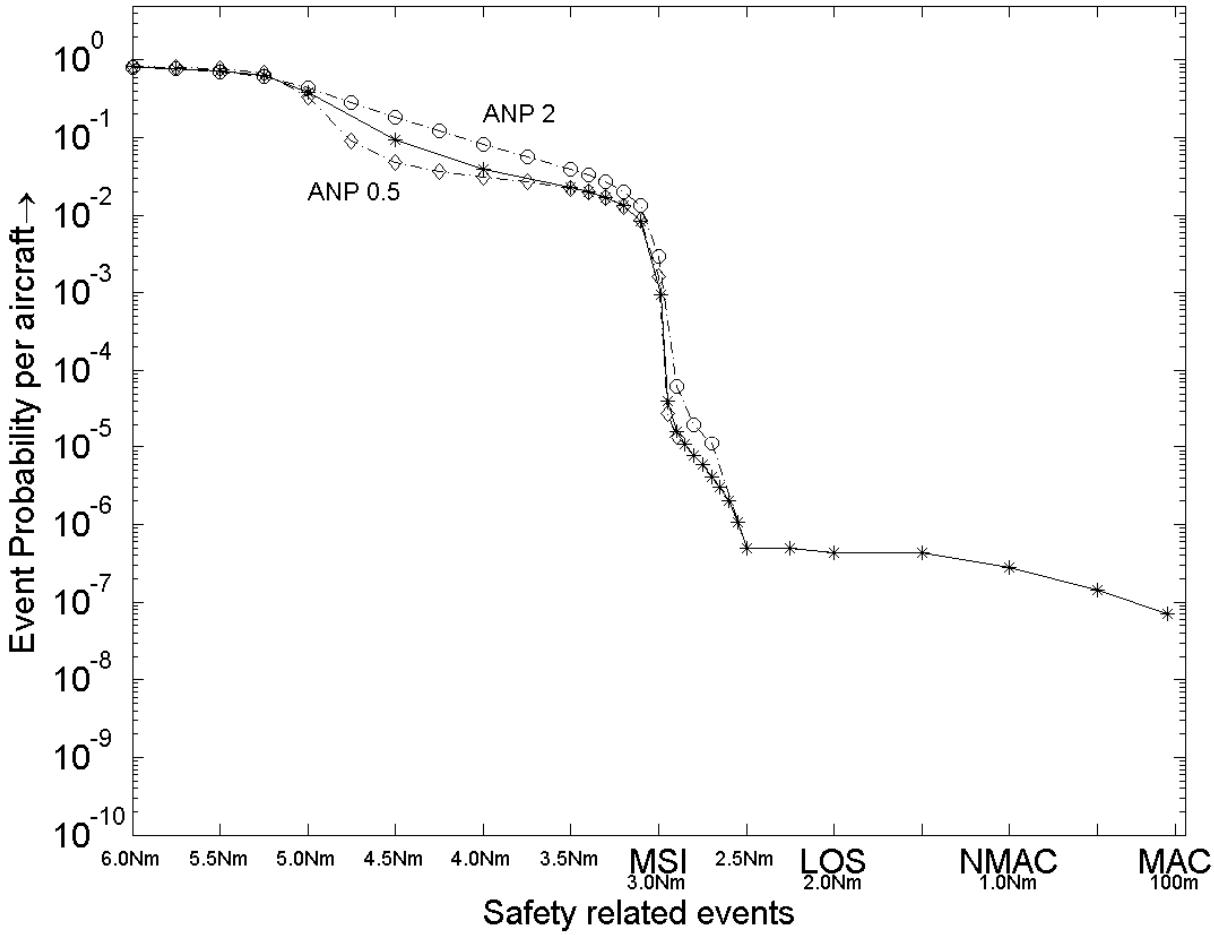

*FIGURE 22: Effect on event probabilities of varying ANP values. * = ANP1, ○ = ANP2, ◊ = ANP0.5.*

Figure 22 shows that a change in ANP value even has a lower impact on the curves than it had for the two aircraft encounter (see Figure 13).

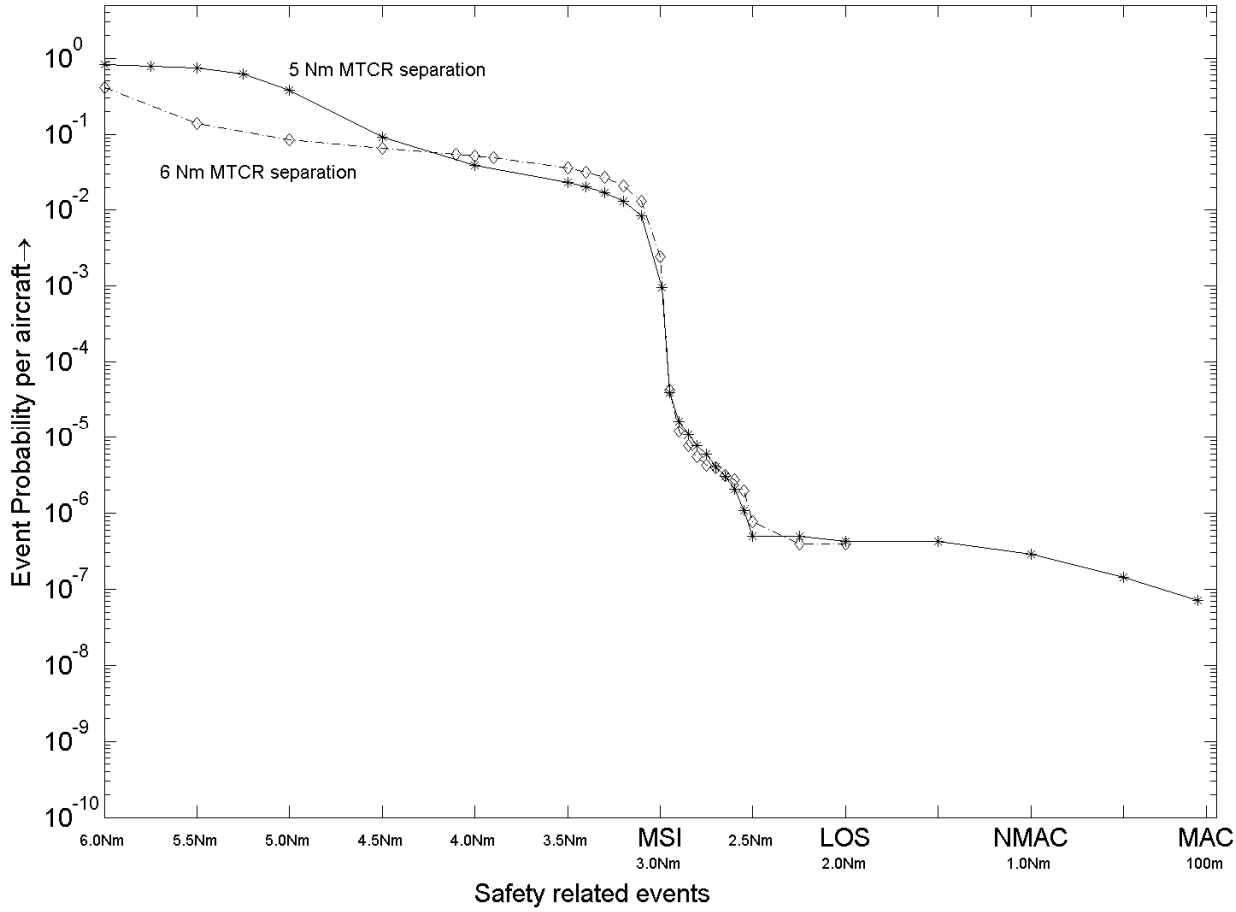

*FIGURE 23: Effect on event probabilities of varying 4D trajectory separation values. * = 5 Nm (baseline), ◊ = 6 Nm.*

Figure 23 shows that an increase of MTCR separation value from 5 Nm to 6 Nm has some impact on the curves. However the sharp reduction that starts to work around MSI is hardly affected. Hence from a safety risk perspective increasing the MTCR separation value does not have a significant impact.

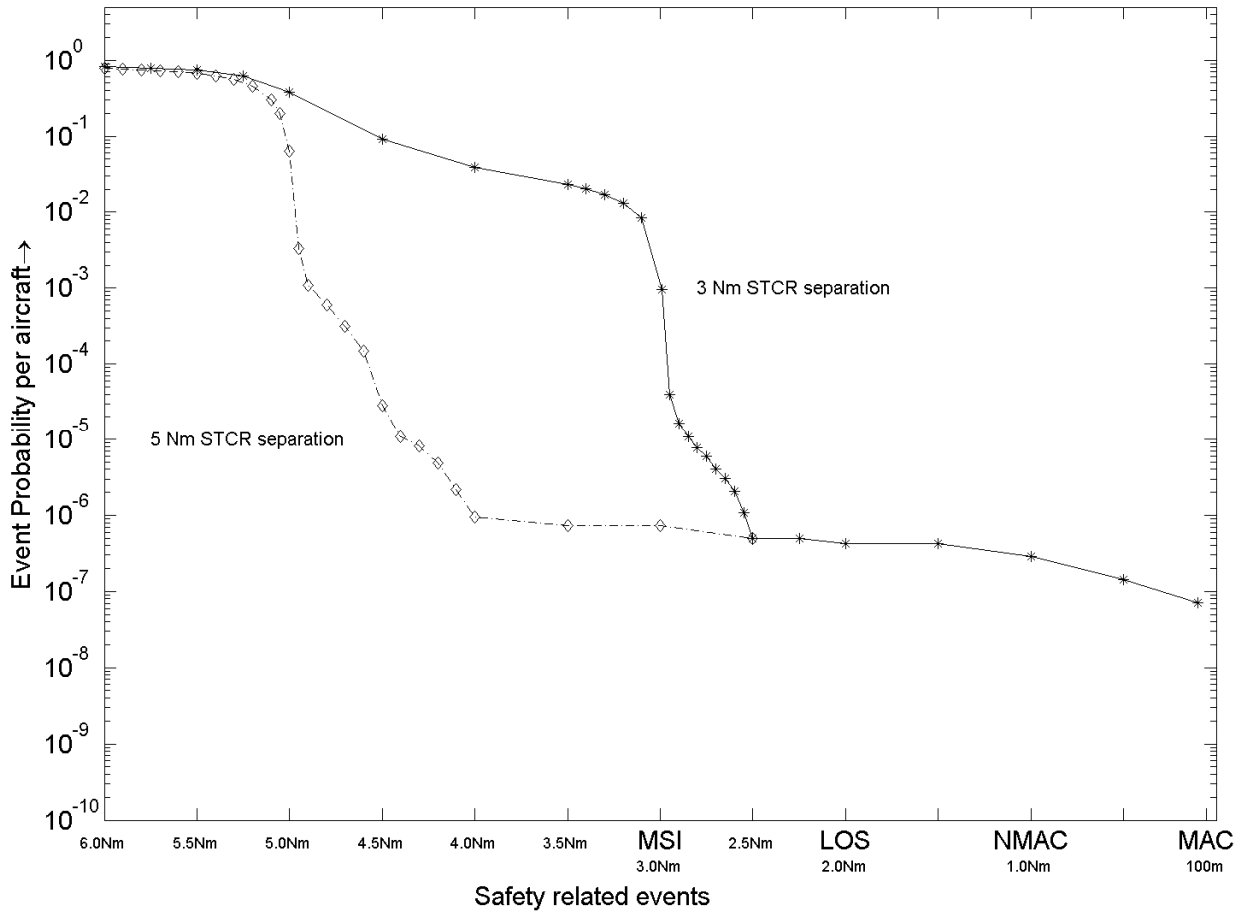

*FIGURE 24: Effect on event probabilities of varying STCR separation values. * = 3 Nm (baseline), ◊ = 5 Nm.*

Figure 24 shows that setting STCR separation value back from 3 Nm to current 5 Nm has a large impact on the curves. The sharp reduction that worked around 3 Nm is now already working around 5 Nm.

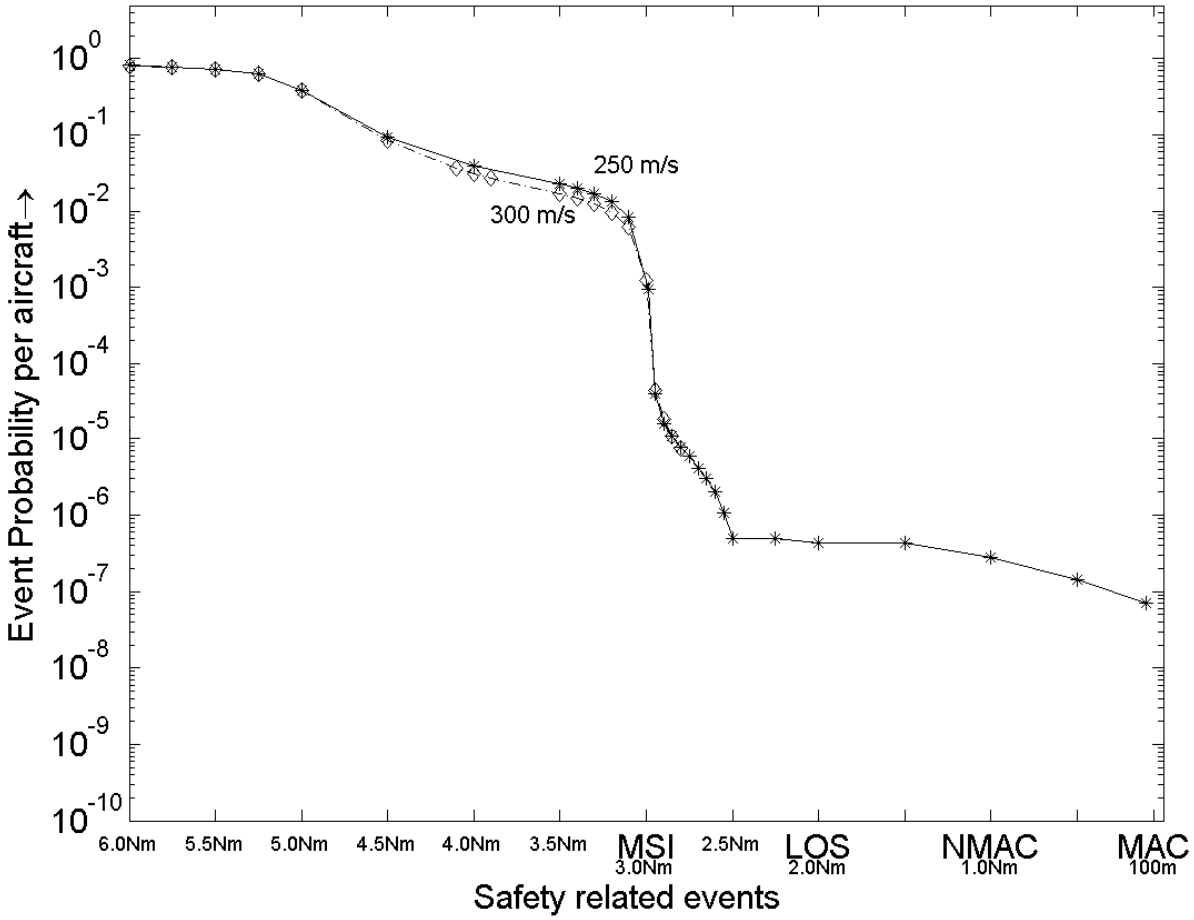

*FIGURE 25: Effect on event probabilities of varying Groundspeed values. * = 250 m/s (baseline), ◊ = 300 m/s.*

The curves in Figure 25 show that the sensitivity to groundspeed does not play a significant factor.

7 Dense random traffic

7.1 Dense random traffic encounter scenario

The third encounter scenario artificially simulates A^3 equipped aircraft flying randomly through a virtually unlimited airspace. In order to accomplish this, the virtually unlimited airspace is filled up with packed containers. Within each container a fixed number of seven aircraft (i = 2, .., 8) fly at arbitrary position and in arbitrary direction at a ground speed of 250 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, and for aircraft that pass the boundary of a container we apply the Periodic Boundary Condition (PBC) approach, e.g. [Rapaport, 2004]. 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. By changing container size we can vary traffic density. In order to avoid that an aircraft experiences a conflict with its own copy in a neighboring container, the size of a container should not become too small.

Our baseline traffic density value is selected to be 4 times the level of one of the busiest en-route sectors in Europe in 1999. This is about 3 times the busiest traffic density in 2005. Based on a data set of European air traffic that has been collected for a busy day in July 1999, the highest aircraft density reference point is a number of 17 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 aircraft per Nm^3. Multiplied by 4 yields our baseline traffic density of 0.0128 aircraft per Nm^3. The latter is 12.8 times the highest traffic density that has been considered in the example of [Andrews et al., 2005, 2006] and 1.6 times the highest traffic density considered for AMFF [Blom, ATC-Q2009].

For the MC simulation of baseline traffic density, i.e. 0.0128 aircraft per Nm^3, we assume for the MC simulations that all 8 aircraft fly on the same flight level (FL) within the container. For the baseline traffic density, this yields 8 aircraft per 62Nm×62Nm×1000ft. Hence, in the MC simulations, we use a 62Nm×62Nm horizontal container size.

Because the initial conditions of seven of the eight aircraft are random, there will be serious short term as well as medium term conflicts in the beginning. Hence for each initial condition, we give the A^3 ConOps a time period of 10 minutes to organize the given traffic situation in line with its concept of operation. Only after this 10 minutes convergence time, we start to measure safety related events, during a period of 10 minutes.

The parameter values considered are specified in Table 11. This includes a random traffic density parameter, which is set at a baseline value 3x as high as a busy sector in 2005, and at a value 6x as high for sensitivity analysis. The latter we simulated by reducing the size of the Periodic Boundary Condition (PBC) by a factor $\sqrt{2}$ in each horizontal direction. The column Id refers to the parameter scenario number in Table 8. For each parameter setting, both light standard MC and IPS [Blom, CDC2006, CRC2007] are conducted. The choice for IPS is because HHIPS remains to be developed for handling multiple aircraft scenarios (see Section 3).

TABLE 11. Parameter value scenarios simulated, MC types and time durations of the computations on two Dell precision T7500

Parameter value scenario	**Figure**	**Standard MC**		**IPS**	
		# of runs	**Duration**	**# of particles**	**Duration**
Baseline	26, 27	3.56 thousand	1 hour	120 thousand + 45 x 10 thousand	42 hours + 138 hours
6x high 2005	26	0.5 thousand	< 1 hour	24 thousand + 20 x 2 thousand	44 hours + 108 hours
STCR	27	110 thousand	31 hours	24 x 10 thousand	64 hours

The total duration of using both Dell machines for the running of simulations for dense random traffic scenarios amounts 430 hours, which comes down to running the two Dell computers 18 days full time. A similar amount of days was needed for the preparation of the simulations (including testing of software adaptations) and for the evaluation and documentation of the simulation results obtained. Comparison of the standard MC and IPS based simulation results are presented and discussed in [iFly D7.2g]. In this section we focus on what the combined result means for the A^3 ConOps.

7.2 Simulation results

The simulation results are shown in Figures 26 and 27. The results in Figure 26 show that for the baseline random traffic scenario, the effectiveness of the A^3 model follows the RNP1 kind of behaviour until it reaches MSI level. Subsequently, the A^3 model produces a factor 10^5 or more improvement between MSI and LOS. This A^3 model behaviour in resolving conflicts is similar to the behaviour seen for the eight-aircraft encounter scenario.

It is remarkable that in none of the rare event simulations a single event has been counted in which the miss distance was lower than 2.0 Nm. The 2.0 Nm value has been counted only once, and this was for the 6x high 2005 scenario. Because we used only 44 thousand particles for the evaluation of this scenario, this means that the speed-up of the IPS approach has been working well. Although for the 3x high 2005 scenario we used an order in magnitude more particles this 2.0 Nm level has even not been reached. However, it should be expected that also for random traffic scenarios there will be some level at which the ASAS dependability values will start to play a role. Also for two aircraft encounters we have seen that this level can be assessed using HHIPS, but not by IPS. Because HHIPS remains to be extended for its application to multiple a/c encounters, this could not yet be assessed through simulations.

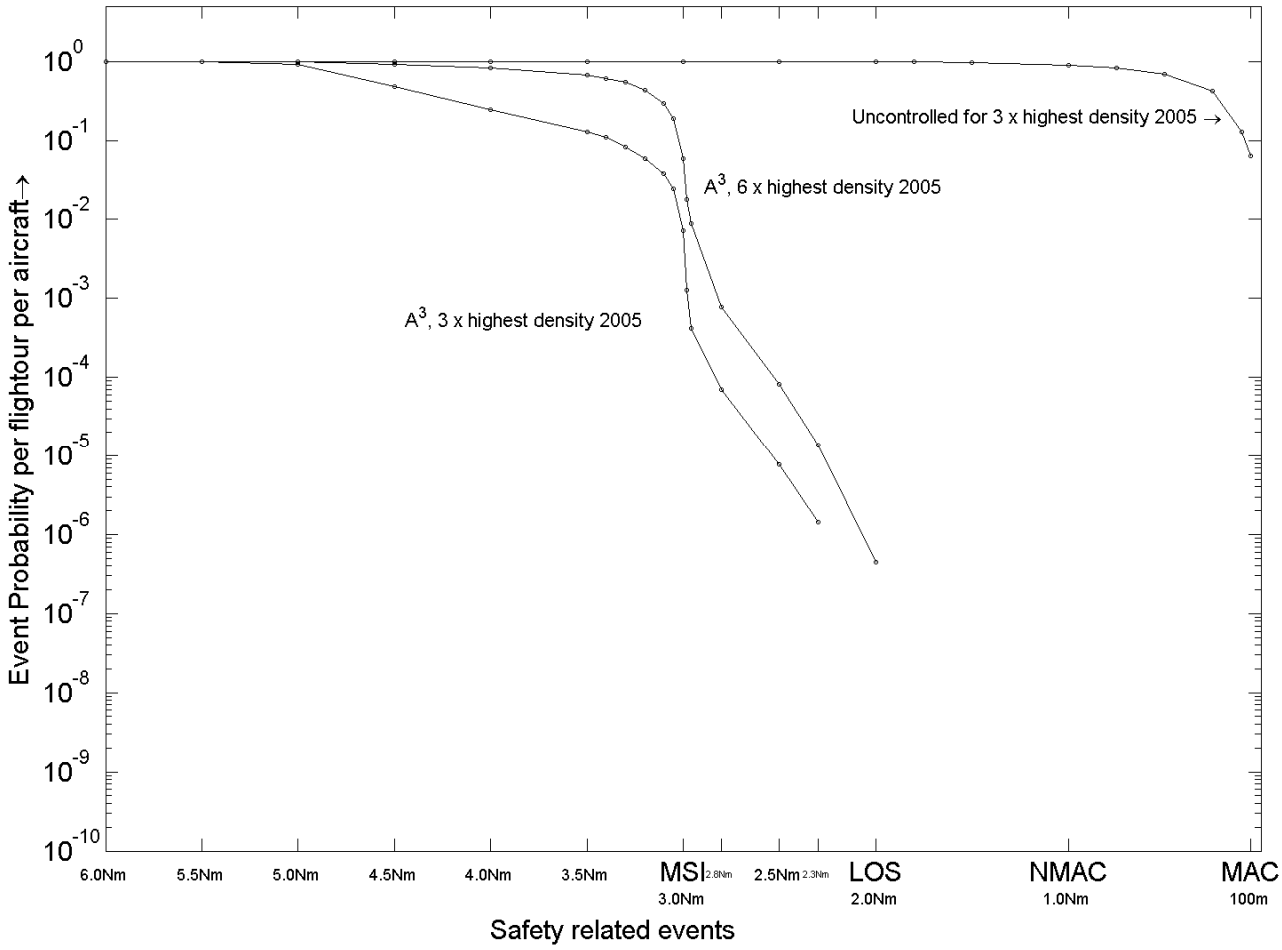

FIGURE 26: Estimated event probability per aircraft per flighthour for random traffic under A^3 model control and uncontrolled. Traffic densities are 3x and 6x high en-route traffic density in 2005.

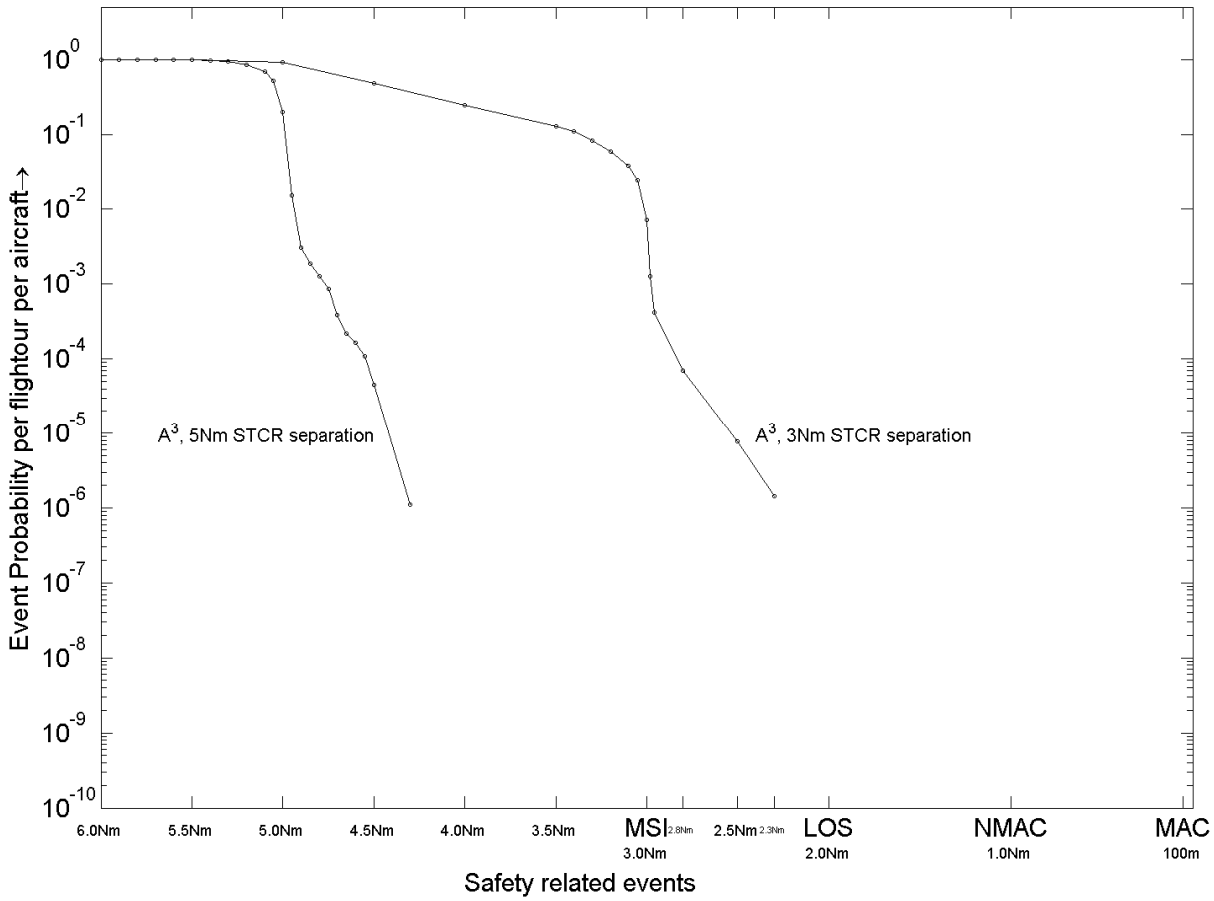

FIGURE 27: Estimated event probability per aircraft per flighthour for random traffic under A^3 model control. Traffic densities is 3x high en-route traffic density in 2005. Left curve is for STCR separation of 5 Nm, right curve for STCR separation of 3 Nm (baseline).

Figure 27 shows that setting the STCR separation value back from 3 Nm to current 5 Nm has a large impact on the curves. Figure 27 shows that the sharp reduction that worked around 3 Nm is now already working around 5 Nm. Although a similar behavior has been seen for the eight aircraft encounter, it is remarkable to see that this also works for very high random traffic.

In view of the very good results obtained for the A^3 ConOps with 5 Nm STCR separation, Figure 28 combines this result with an estimated curve for the effect of baseline dependability of ASAS related systems. First the new curve is obtained by running MC simulations with initial condition that ADS-B global is down. Subsequently this curve is copied at a factor 10^{-6} lower values to complete the curve for the A^3 ConOps.

Figure 28 also shows a current reference point in the form of probability values per flighthour that in NATS controlled airspace the miss distance between aircraft underscores 66% of the applicable minimum separation criteria [NATS, 2011]. For the 3× highest denstiy in 2005, the A^3 ConOps with a 5 Nm STCR separation minimum, is doing much better than the [NATS, 2011] values for the current operation.

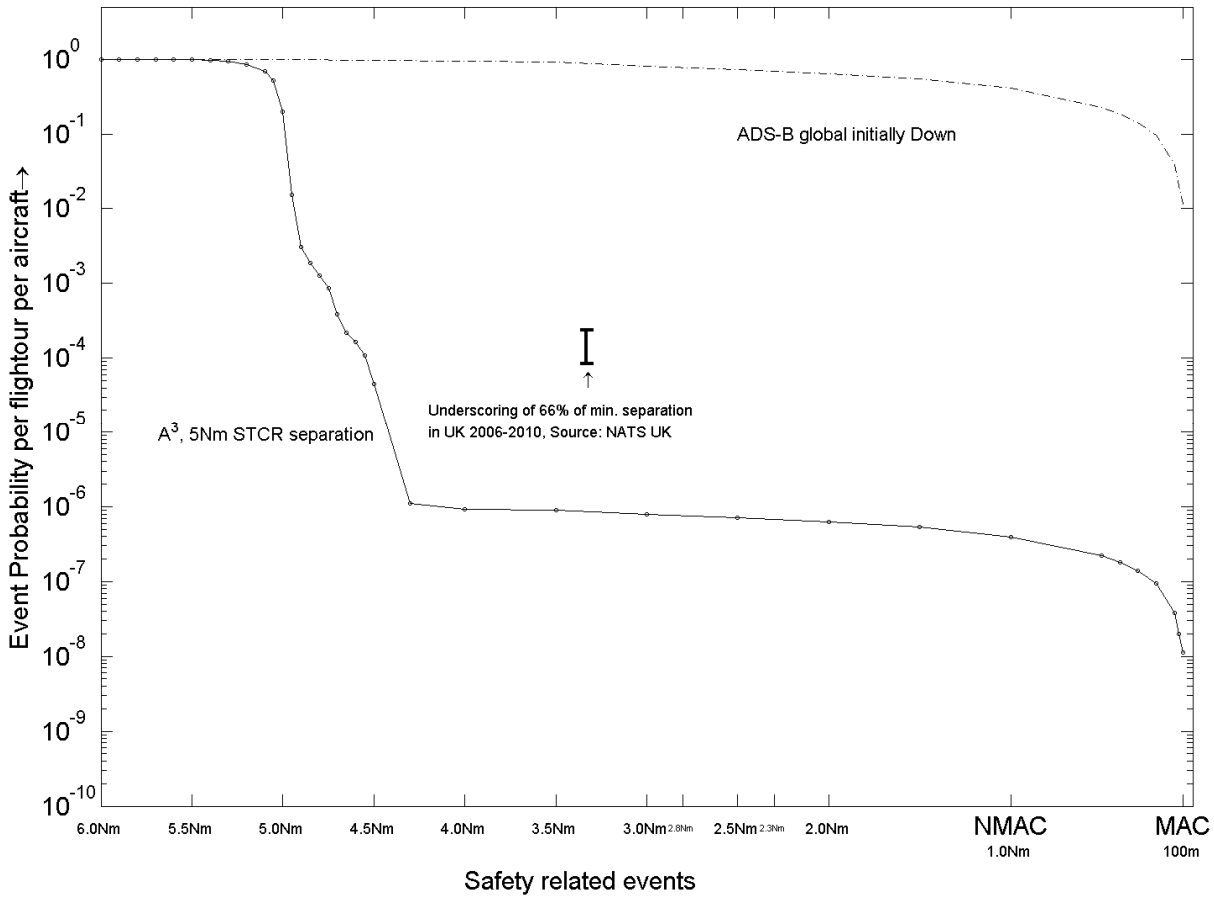

FIGURE 28: Estimated event probability per aircraft per flighthour for random traffic under A³ model control at traffic demand of 3x high en-route traffic demand in 2005. The dashed curve at the top is obtained through running standard MC simulations for the A³ ConOps model under the initial condition that ADS-B Global is Down. nd uncontrolled. This curve has been used to construct a completion of the line curve for miss distance values below 4Nm.

7.3 Comparison against future TLS

In [iFly D7.1a] a Target Level of Safety (TLS) value has been derived for an advanced airborne self separation operation that has to accommodate X times more traffic demand than was applicable in the year 2000. This derivation uses the TLS value specified by [ICAO, Annex 11, 2003] as starting point.

[ICAO Annex 11, 2003], Attachment B states in section 3.2.1: "Where 'fatal accidents per flight hour' is considered to be an appropriate metric, a target level of safety (TLS) of 5×10^{-9} fatal accidents per flight hour per dimension should be applied for determining the acceptability of future en-route systems that will be implemented after the year 2000." It is quite important to notice that this TLS should apply when Airborne Collision Avoidance System (ACAS) is not taken into account. Apart of this ACAS aspect, the rationale used

behind the argumentation in developing this TLS value is well developed, and this en-route TLS has regularly been adapted to traffic growth by ICAO's Review of General Concept of Separation Panel (RGCSP) [Parker, 1996; DNV, 2005]. For example, prior to 2000, the TLS was a factor four higher, i.e. 2×10^{-8} fatal accidents per flight hour and per dimension, which equals 6×10^{-8} fatal accidents per flight hour. Based on accident statistics over 1980-1999, the estimated mid-air fatal accident risk is 3.35×10^{-8} fatal mid-air accidents per flight [Hybridge D2.2, 2003]. If we assume one flight takes about 2 hours, this comes down to about 1.7×10^{-8} fatal mid-air accidents per flight hour, which is about a factor 3.5 lower than the TLS value posed by ICAO during that period.

Part of the explanation of this factor 3.5 is that the ICAO en-route mid-air collision safety target setting does not take airborne based safety nets into account. This may lead to the undesired situation that the ICAO en-route mid-air collision TLS provides no incentive to improve airborne based safety nets, and to improve the collaboration between ground-based and airborne-based safety nets. For advanced developments of Airborne Separation Assistance System (ASAS) and further development of ACAS there is an obvious need to take this into account when defining future TLS values for mid-air collision. In [RESET D6.1, 2007] it has been argued that this needs to be changed in order to give airborne self separation a fair chance.

Taking into account a traffic growth factor X since 2000, whereas the frequency of fatal accident headlines in the news may not increase, then the TLS should be reduced by this same factor X. This means that iFly should adopt a TLS of $3\times5\times10^{-9}/X$ fatal accidents per aircraft flight hour, and this should apply without taking ACAS into account. Moreover, ACAS should at least yield a factor 3.5 extra reduction in fatal accident risk [iFly D7.1a].

The 3x high 2005 traffic demand corresponds to 4x high 1999 traffic demand. In neglecting the one year difference, we assume X=4. This means that the TLS to be adopted in Figure 26 is $3\times5\times10^{-9}/4 = 3.75\times10^{-9}$ fatal accidents per aircraft flight hour, and this should apply without taking ACAS into account. Moreover, ACAS should at least yield a factor 3.5 extra reduction in fatal accident risk [iFly D7.1a].

The derived TLS value incorporates all three collision types (i.e. 2x horizontal + 1x vertical). Because the simulated scenario in Figure 28 covers only two of these three directions, the applicable TLS value is 2.5×10^{-9}. This means that the estimated curve in Figure 28 points to a factor 5 more safety risk than the derived TLS value. This means that the safety risk remains to be improved by an extra factor 5. One way to realize such a factor 5 lower TLS value is to require the probability of Global ADS-B down to be a factor 5 lower than the 10^{-6} adopted so far. An alternative way to realize such an extra factor 5, is to demonstrate that future ACAS provides this factor 5 extra improvement, i.e. future ACAS should provide a safety improvement factor of 5x3.5 = 17.5.

8 Concluding remarks

In [iFly D1.3] an advanced airborne self separation operation for en-route airspace has been developed under the name A^3 ConOps (Concept of Operations). The key question posed by the iFly project is how much en-route traffic demand can this A^3 ConOps safely accommodate? In order to address this question, a multi-agent model of the A^3 ConOps has been developed, which includes human and technical agents, their interactions and both the nominal and non-nominal aspects of the operation. Subsequently this model has been used to run rare event Monte Carlo simulations for the following three encounter scenarios:

1. Two aircraft head-on encounter
2. Eight aircraft head-on encounter
3. Random traffic scenarios

The MC simulation results obtained for these scenarios show that the A^3 ConOps model works very well for all scenarios considered. More specifically, the results show that the A^3 ConOps model may safely accommodate 3x to 6x the traffic demand of a very busy en-route sector in 2005.
Parameter sensitivity analysis shows that the results are pretty insensitive to RNP level, Crew response time, Medium Term separation minimum and Groundspeed. Significant sensitivity has been identified regarding ASAS dependability level and the tactical separation minimum. For the ASAS dependability this means that it should be 10x more dependable than what was needed for using the AMFF ConOps over the Mediterranean. For the Tactical separation minimum there appears no need to reduce the current value of 5 NM minimum tactical separation to the 3 NM proposed in [iFly D1.3].

Hence the answer to the fundamental question is: advanced Airborne Self Separation can safely accommodate 3x high 2005 traffic demand, under the following conditions:

- The dependability of ASAS support systems has to be of a high level. From the rare event MC simulation results safety objectives for the dependability parameters of the various sub-systems have been identified.
- The most demanding safety objective concerns the probability of ADS-B Global being down: it must be 5 times better than what has been identified as being needed for the Autonomous Mediterranean Free Flight. If the safety objectives for the ASAS system dependability cannot be realized in practice, then an alternative is to improve future TCAS such that this provides a 5 times higher factor in safety improvement than current TCAS does.

Because iFly project covers the safety evaluation of the early development phase of an advanced airborne self separation ConOps, it is recommended that these findings receive follow-up research in the next A^3 ConOps development and validation phase. Follow-up research should also cover weather influences, incorporation of vertical movements, and further validation of the A^3 model results.

References

[Abe & Yoshiki, 2001] Abe, Y.; Yoshiki, M.. "Collision avoidance method for multiple autonomous mobile agents by implicit cooperation". IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 01). New York, N.Y.: IEEE. November 2001, pp. 1207–1212.

[AIAA, 1998] AIAA, Guide for the verification and validation of computational fluid dynamics simulations, AIAA report G-077-1998, 1998.

[Alexander, 1970] B. Alexander, Aircraft density and midair collision, Proceedings of the IEEE, Vol. 58, 1970, pp. 377-381.

[Andrews et al., 2005] J.W. Andrews, J.D. Welch, H. Erzberger. Safety analysis for advanced separation concepts. Proceedings of USA/Europe ATM R&D Seminar, Baltimore, USA, 27–30 June 2005.

[Andrews et al., 2006] J.W. Andrews, H. Erzberger, J.D. Welch. Safety analysis for advanced separation concepts. ATC Quarterly, Vol. 14, 2006, pp. 5-24.

[Blom, CDC2006] Blom H.A.P., Krystul J., Bakker G.J., A particle system for safety verification of free flight in air traffic, Proc. IEEE Conf. Decision and Control, San Diego, CA, 13-15 December 2006.

[Blom, CRC2007] Blom H.A.P., Krystul J., Bakker G.J., Klompstra M.B., Klein Obbink B, Free flight collision risk estimation by sequential Monte Carlo simulation, Eds: C.G. Cassandras and J. Lygeros, Stochastic hybrid systems; recent developments and research trends, Taylor & Francis/CRC Press, 2007, pp. 249-281.

[Blom, CDC2007] H.A.P. Blom, Bakker G.J., Krystul J., Reachability analysis for large scale stochastic hybrid systems, Proc. IEEE Conference on Decision and Control, December 12-14, 2007, New Orleans, USA.

[Blom, Wiley2009] H.A.P. Blom, G.J. Bakker and J. Krystul, Rare event estimation for a large scale stochastic hybrid system with air traffic application, Chapter in: G. Rubino and B. Tuffin (editors), Rare event simulation using Monte Carlo methods, Wiley, 2009.

[Blom, ATC-Q2009] H.A.P. Blom, B. Klein Obbink, G.J. Bakker, Simulated Safety Risk of an Uncoordinated Airborne Self Separation Concept of Operation, Air Traffic Control Quarterly, Volume 17 (2009) Number 1, pp. 63-93.

[Bujorianu, 2004] M.L. Bujorianu. Extended stochastic hybrid systems. In Proceedings of Hybrid Systems Computation and Control, Eds. O.Mahler, A. Pnuelli, LNCIS number 2993, Springer, Berlin, pages 234–249, 2004.

[Cassandras, 1999] C.G. Cassandras, S. Lafortune. Introduction to Discrete Event Systems, Kluwer Academic Publishers, Boston, 1999.

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

[Cerou et al., 2005] F. Cérou, Del Moral P., Le Gland F., Lezaud P., Limit theorems for the multilevel splitting algorithms in the simulation of rare events. Proc. Winter Simulation Conference, Orlando, USA, 2005.

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

[DNV, 2005] DNV for Eurocontrol, Definition and use of target levels of safety, Task 1 report, TRS 046/04, Revision 3, 13th October 2005.

[Duong &Hoffman, 1997] V.N. Duong and E.G. Hoffman, Conflict resolution advisory service in autonomous aircraft operations, Proc. 16th Digital Avionics Systems Conf., 1997.

[Endoh & Odoni, 1983] S. Endoh and A.R. Odoni, A generalized model for predicting the frequency of air conflicts, Proc. Conf. on Safety Issues in ATM Systems Planning and Design, Princeton, New Jersey, September 1983.

[E-OCVM, 2010] European Operational Concept Validation Methodology (E-OCVM) Version 3.0 Volumes I and II (Annexes), Eurocontrol, February 2010

[Everdij & 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, 2003] 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, pp. 355–360, June 2003.

[Everdij & Blom, 2005] M.H.C. Everdij, H.A.P. Blom. Piecewise deterministic Markov processes represented by Dynamically Coloured Petri Nets, Stochastics, Vol. 77, pp.. 1–29, 2005.

[Everdij & Blom, 2006] M.H.C. Everdij, H.A.P. Blom. Hybrid Petri nets with diffusion that have into mappings with generalised stochastic hybrid processes. . Eds: H.A.P. Blom, J. Lygeros. Stochastic Hybrid Systems: Theory and Safety Critical Applications, LNCIS series, Springer, Berlin, July 2006, pp. 31–64.

[Everdij, PSAM2006] M.H.C. Everdij, H.A.P. Blom, S.H. Stroeve. Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk. Proc, 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), New Orleans, USA, May 2006.

[Everdij, Springer2006] 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. Eds: H.A.P. Blom, J. Lygeros. Stochastic Hybrid Systems: Theory and Safety Critical Applications, LNCIS series, Springer, Berlin, July 2006, pp. 325–350, 2006.

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

[Fiorini & Schiller, 1998] P. Fiorini, Z. Schiller, "Motion planning in dynamic environments using velocity obstacles". The International Journal of Robotics Research, Volume 17 (1998), pp. 760–772.

[Gayraud et al, 2005] B. Gayraud, Nacchia F., Barff J., Ruigrok R.C.J., MFF operational concept, requirements and procedures, Report MFF D220, 2005, www.medff.it/public/index.asp.

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

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

[HYBRIDGE D2.2, 2003] Stochastic analysis background of accident risk assessment for Air Traffic Management by Henk Blom, Bert Bakker, Mariken Everdij, Marco van der Park. Final version 1.1 of 29 July 2003. Available on HYBRIDGE website http://hosted.nlr.nl/public/hosted-sites/hybridge/

[ICAO, 2003] ICAO, Airborne separation assistance system (ASAS) circular, Draft, version 3, SCRSP, WGW/1 WP/5.0, International Civil Aviation Organization, May 2003.

[ICAO Annex 11, 2003] ICAO, International Standards and Recommended Practices – Air Traffic Services, Annex 11, 13th edition, November 2003.

[iFly D1.3] iFly Deliverable D1.3, Autonomous Aircraft Advanced (A^3) ConOps, written by Isdefe (Gustavo Cuevas, Ignacio Echegoyen, José García García), Honeywell (Petr Cásek, Claudia Keinrath, …,…), NLR (Frank Bussink), and Utartu (Aavo Luuk), January 2010. Available on iFly website http://ifly.nlr.nl/

[iFly D2.2] iFly Deliverable D2.2, Situation Awareness, Information, Communication and Pilot Tasks of under autonomous aircraft operations, John Wise, Claudia Keinrath, Fleur Pouw, Amel Sedaoui, Vincent Gauthereau and Aavo Luuk, Version 1.3, 8 April 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D3.2] iFly Deliverable D3.2, Report on timely prediction of complex conditions for en-route aircraft, by M. Prandini, L. Piroddi, S. Puechmorel, P. Cásek and S.L. Brázdilová. Final version 1.2 of 16

May 2011.

[iFly D5.3] iFly Deliverable D5.3, Report on advanced conflict resolution mechanisms for A^3 ConOps, by E. Siva, J.M. Maciejowski, G. Chaloulos, J. Lygeros, G. Roussos, K.Kyriakopoulos. Final version 1.0 of 23 August 2011.

[iFly D7.1a] iFly Deliverable D7.1a, Accident risk and flight efficiency of A^3 operation -Scoping and safety target - by H.A.P. Blom, Version 1.1 of 3 February 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D7.1b] iFly Deliverable D7.1.b, Hazard Identification and Initial Hazard Analysis of A^3 ConOps based operation, H.A.P. Blom, G.J. Bakker, M.B. Klompstra and F.J.L. Bussink, Version 0.8, September 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D7.1c] iFly Deliverable D7.1c, Report on Petri Net modelling of the A^3 operation by G.J. Bakker and H.A.P. Blom. Version 0.6 of 28 Sep 2010

[iFly D7.2a] iFly Deliverable D7.2a, Review of risk assessment status for air traffic. Editors: H.A.P. Blom, J. Krystul, P. Lezaud and M.B. Klompstra, Version 1.0 of 14 Jan 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D7.2b] iFly Deliverable D7.2b, Trans-dimensional simulation for rare-events estimation on stochastic hybrid systems by N. Kantas and J.M. Maciejowski, Version 1.0 of 1 May 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D7.2c] iFly Deliverable D7.2c, Interim report on importance sampling of multi aircraft encounter geometries - Air traffic complexity and the interacting particle system method: an integrated approach for collision risk estimation by Maria Prandini, Henk A.P. Blom, Bert G.J. Bakker. Version 0.5 of 8 Apr 2011

[iFly D7.2d] iFly Deliverable D7.2d, Periodic Boundary Condition in Simulating Large Scale Airborne Self Separation Airspace by A. Goswami, G.J. Bakker, H.A.P. Blom, Version 1.0 of 11 April 2010

[iFly D7.2e] iFly Deliverable D7.2e, Rare event estimation for a large scale stochastic hybrid system with air traffic application - IPS extension to large hybrid systems - by H.A.P. Blom, G.J. Bakker and J. Krystul. Version 0.6 of 28 Jan 2009. Available on iFly website http://ifly.nlr.nl/

[iFly D7.2f] iFly Deliverable D7.2f, Sensitivity analysis in Monte Carlo simulation based rare event estimation, by M.B. Klompstra, G.J. Bakker and H.A.P. Blom, Version 1.3 dated 22 March 2011

[iFly D7.2g] iFly Deliverable D7.2g, Final report on Monte Carlo speed-up studies, by H.A.P. Blom, G.J. Bakker. Version 0.5 of 22 August 2011.

[iFly D8.1] iFly Deliverable D8.1, A^3 ConOps refinement. Editor: L. Biescas, Final draft of 23 May 2011

[iFly D9.1] iFly Deliverable D9.1, Operational Services and Environmental Description (OSED) of Airborne Self-Separation Procedure (SSEP), by E. Gelnarová, P. Cásek, August 2009.

[Jensen, 1992] K. Jensen. Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use, Vol. 1, Springer, London, UK, 1992.

[KleinObbink, 2005] B. Klein Obbink. MFF airborne self separation assurance OSED, Report MFF R733D, April 2005, available at http://www.medff.it/public/index.asp.

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

[Krystul, 2006] J. Krystul. Modelling of stochastic hybrid systems with applications to accident risk assessment, PhD Thesis, Twente University, 2006.

[Krystul & Blom, 2005] J. Krystul, H.A.P. Blom. Generalised stochastic hybrid processes as strong solutions of stochastic differential equations, Hybridge Report D2.3, 2005, see http://www.nlr.nl/public/hosted-sites/hybridge/.

[Krystul et al., 2007] J. Krystul, H.A.P. Blom and A. Bagchi, Stochastic hybrid processes as solutions to stochastic differential equations, Eds: C.G. Cassandras and J. Lygeros, Stochastic hybrid systems: Recent developments and research trends, CRC Press, 2007, pp. 15-45.

[Labeau et al., 2000] 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, pp. 219–254, 2000.

[Maracich, 2005] Maracich F., Flying free flight: pilot perspective and system integration requirements, Proc. 24th DASC, Washington, 2005.

[NASA, 1999] 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.

[NASA, 2004] NASA. DAG-TM Concept element 5 en-route free maneuvering for user-preferred separation assurance and local TFM conformance operational concept description, AATT Project Milestone 8.503.10, NASA Airspace Systems Program Office, Washington D.C.

[NATS, 2011] NATS presentation at FAA/Eurocontrol AP15 meeting, Washington DC, March 8-10, 2011.

[Parker, 1996] I. Parker, The history of the derivation and application of Target Levels of Safety, Eurocontrol workshop, 14/15 March 1996.

[Pola et al., 2003] 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), Saint-Malo, Brittany, France, 2003.

[Rapaport, 2004] D.C. Rapaport, The art of molecular dynamics simulation, Cambridge University Press, 2004.

[RESET D6.1, 2007] H. Blom, M. Everdij, B. Van Doorn, D. Bush and K. Slater, Existing safety assessment methods versus requirements, RESET project report D6.1 for EC-DG-TREN, Version 0.6, September 2007.

[RTCA, 1995] RTCA, Final report of RTCA Task Force 3; Free Flight implementation, RTCA Inc., Washington DC, October 1995.

[RTCA, 2002] RTCA, DO-242a, Minimum aviation system performance standards for ADS-B, issued 25th June 2002

[Scholte, 2005] J.J. Scholte, B. Klein Obbink, Self separation assurance ASOR, MFF report R734L, edition 0.9, June 2005.

Appendix A. A³ model specification formalism

A.1 Petri Net formalism

For the modelling of accident risk of safety-critical operations in nuclear and chemical industries, the most advanced approaches use Petri nets as model specification formalism, and stochastic analysis and Monte Carlo simulation to evaluate the specified model, e.g., see [Labeau et al., 2000]. Since their introduction as a systematic way to specify large discrete event systems that one meets in computer science, Petri nets have shown their usefulness for many practical applications in different industries, e.g., see [David & Alla, 1994]. Various Petri net extensions and generalisations and numerous supporting computer tools have been developed, which further increased their modelling opportunities. Nevertheless, literature on Petri nets appeared to fall short for modelling the class of General Stochastic Hybrid Systems (GSHS) [Bujorianu, 2004] that was needed to model air traffic safety aspects well [Pola et al., 2003].

[Cassandras, 1999] provide a control systems introduction to Petri nets and a comparison with other discrete eventmodelling formalisms like automata. Both Petri nets and automata have their specific advantages. Petri net is more powerful in the development of a model of a complex system, whereas automata are more powerful in supporting analysis. In order to combine the advantages offered by both approaches, there is need for a systematic way of transforming a Petri net model into an automata model. Such a transformation would allow using Petri nets for the specification and automata for the analysis. For a timed or stochastic Petri net with a bounded number of tokens and deterministic or Poisson process firing, such a transformation exists [Cassandras, 1999]. In order to make the Petri net formalism useful in modelling air traffic operations, we need an extension of the Petri net formalism including a one-to-one transformation to and from GSHS. Everdij and Blom [2003, 2005, 2006] have developed such extension in the form of (Stochastically and) Dynamically Coloured Petri Net, or for short (S)DCPN.

[Jensen, 1992] introduced the idea of attaching to each token in a basic Petri net (i.e., with logic transitions only), a colour which assumes values from a finite set. Tokens and the attached colours determine which transitions are enabled. Upon firing by a transition, new tokens and attached colours are produced as a function of the removed tokens and colours. [Haas, 2002] extended this colour idea to (stochastically) timed Petri nets where the time period between enabling and firing depends of the input tokens and their attached colours. In [Haas, 2002] and [Jensen, 1992] a colour does not change as long as the token to which it is attached remains at its place. [Everdij and Blom, 2003, 2005] defined a Dynamically Coloured Petri Net (DCPN) by incorporating the following extensions: (1) a colour assumes values from a Euclidean state space, its value evolves as solution of a differential equation and influences the time period between enabling and firing; (2) the new tokens and attached colours are produced as random functions of the removed tokens and colours. An SDCPN extends an DCPN in the sense that colours evolve as solutions of a stochastic differential equation [Everdij & Blom, 2006].

This appendix explains how the SDCPN formalism has been used to develop a MC simulation model of the A^3 operation, with focus on the syntactical side. Within the Hybridge project the same formalism has been used to develop a MC simulation model of the Autonomous Mediterranean Free Flight (AMFF) operation [KleinObbink, 2005], and subsequently to use this for collision risk estimation [Everdij & Blom, 2003, 2005, 2006]. Similarly as applied with AMFF, for the development of a Petri net model of the A^3 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 representing the A^3 operation sufficiently well.

A.2 Specification of Development of a Petri Net Model

In using the (S)DCPN formalism [Everdij & Blom, 2003, 2005, 2006] in modelling more and more complex multi-agent hybrid systems, it was found that the compositional specification power of Petri nets reaches its limitations. More specifically, the following problems were identified:

1. 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.
2. 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.
3. The number of interconnections between the different low level Petri nets tends to grow quadratically with the size of the Petri net.

[Everdij, Springer 2006] explained which Petri net model specification approaches from literature solve problem 1, and developed novel approaches to solve problems 2 and 3. Together, these approaches are integrated into a compositional specification approach for SDCPN, which is explained below.
In order to avoid problem 1, 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). 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 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.

- Interaction Petri Net (IPN) from one (or more) transition(s) in one LPN to one (or more) transition(s) in another LPN.

In order to avoid problems 2 and 3, high level interconnection arcs have been introduced that allow, with well-defined meanings, arcs to initiate and/or to end on the edge of the box surrounding an LPN [Everdij, Springer 2006]. 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.

A.3 High Level Interconnection Arcs

As an illustration of how high level interconnection arcs avoid duplication of arcs and transitions within an LPN and duplication of arcs between LPNs, we give three examples of these high level interconnection arcs. See [Everdij, Springer 2006] for a complete overview of these high level interconnection arcs.

In the first example, Figure A.1, an enabling arc starts on the edge of an LPN box and ends on a transition in another LPN box, means that enabling arcs initiate from all places in the first LPN and end on duplications of this transition in the second LPN. The duplicated transitions should have the same guard or delay function and the same firing function and their input places should have the same colour type. This high level interconnection arc is not defined for inhibitor or ordinary arcs instead of enabling arcs.

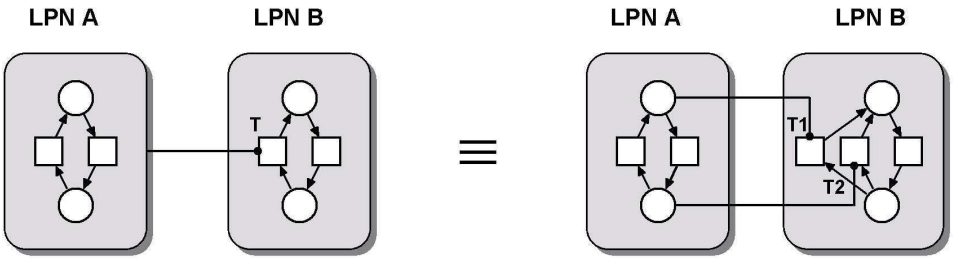

FIGURE A.1: High level enabling arc starts at the edge of an LPN box.

In the second example, Figure A.2, an enabling arc ends on the edge of an LPN box. This means that for each transition in the receiving LPN a copy of this enabling arc should be in place. Figure A.2 shows an example of this high level interconnection arc. This type of high level arc can also be used with inhibitor arcs instead of enabling arcs. It cannot be used with ordinary arcs, due to the restriction that the number of tokens in an LPN should remain the same.

In the third example, Figure A.3, an ordinary arc starts on the edge of an LPN box and ends on a transition inside the same box. This means that ordinary arcs start from all places in the LPN box to duplications of this transition. The duplicated transitions should have the same guard or delay function and the same firing function and their set of input places should have the same set of colour types. Figure A.3 illustrates how this avoids both the duplication of transitions and arcs within an LPN, and the duplication of arcs between LPNs.

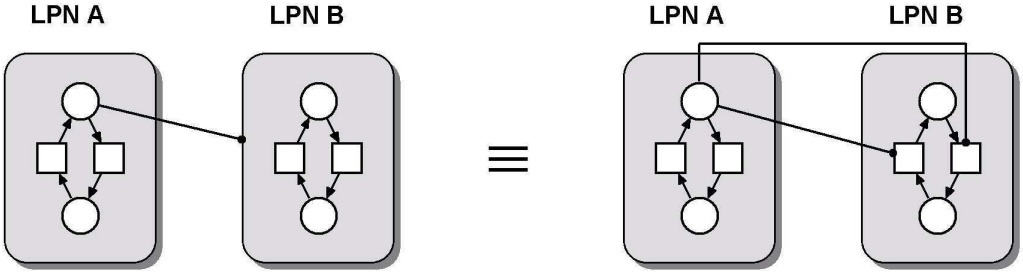

FIGURE A.2: High level enabling arc ends at the edge of an LPN box.

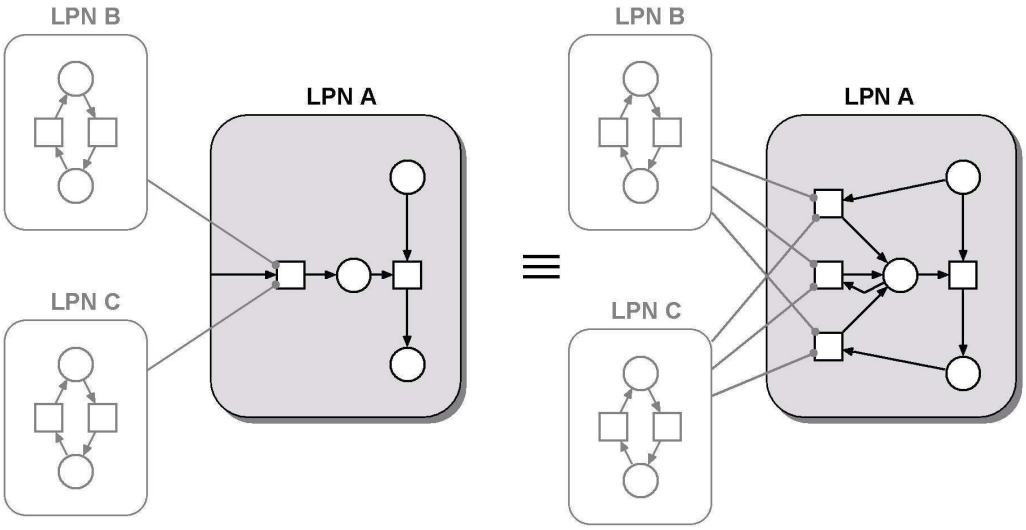

FIGURE A.3: High level ordinary arc starts on the edge of an LPN box and ends on a transition inside the same LPN box.

This page is intentionally left blank.

Appendix B. A^3 Model Parameters

This appendix lists for each agent the parameters that apply for each LPN. Also baseline parameter values and sources are given.

Agent	LPN	Parameter	Explanation	Value	Source
Aircraft	Engine System	$\mu^{\text{fail}}_{\text{Engine}}$	Mean duration of *Engine Failure* $\rightarrow$ *No engine failure*	1 hr	Expert
		$p^{\text{fail}}_{\text{Engine}}$	Probability of *Engine Failure*	1/6000	Expert
	Emergency Mode	$\mu^{\text{emer}}_{\text{OES}}$	Mean duration of *Emergency* $\rightarrow$ *No Emergency*	1 hr	MFF Workshop (MFFW)
		$p^{\text{emer}}_{\text{OES}}$	Probability of *Emergency*	1/6000	MFFW
Pilot flying	Current Goal	$m^{\text{goals}}_{\text{PF}}$	Total number of goals of PF	7	Model
		$m^{\text{failures}}_{\text{PF}}$	Total number of failures in case of 'Emergency actions' goal for PF	6	Model
	Goal Memory	$m^{\text{goals}}_{\text{PF}}$	Total number of goals of PF	7	Model
		$m^{\text{failures}}_{\text{PF}}$	Total number of failures in case of 'Emergency actions' goal for PF	6	Model
	Task Performance$_{\text{PF}}$ Goal 2: Emergency Actions	μ^{MD}_{PF}	Mean duration of *Monitoring & Decision* $\rightarrow$ *Coordination*, Duration parameter of *Monitoring & Decision* $\rightarrow$ *Execution*	10 s	Expert
		μ^{Coord}_{PF}	Mean duration of *Coordination* $\rightarrow$ *Monitoring & Decision*	5 s	Expert
		μ^{ExMon}_{PF}	Mean duration of *Execution Monitoring* $\rightarrow$ *Monitoring & Goal Prioritisation*	20 s	Expert
		μ^{MonGP}_{PF}	Mean duration of *Monitoring & Goal Prioritisation* $\rightarrow$ *End Task*	10 s	Expert

Agent	LPN	Parameter	Explanation	Value	Source
Pilot flying (Continued)	Task Performance$_{\text{PF}}$ Goal 3: Conflict Resolution	$\mu^{T_d^1}$	Mean decision delay time in case Short Term Conflict	5.7 s	RESET
		$\mu^{T_d^2}$	Mean decision delay time in case Medium Term Conflict	30 s	Expert
		μ_{PF}^{MD}	Mean duration of *Monitoring & Decision* $\rightarrow$ *Coordination*	∞	Expert
		μ_{PF}^{Coord}	Mean duration of *Coordination* $\rightarrow$ *Monitoring & Decision*	0 s	Expert
		μ_{PF}^{ExMon3}	Mean duration of *Execution Monitoring* $\rightarrow$ *Monitoring & Goal Prioritisation*	14.7 s	RESET
		μ_{PF}^{MonGP3}	Mean duration of *Monitoring & Goal Prioritisation* $\rightarrow$ *End Task*	10 s	Expert

Agent	LPN	Parameter	Explanation	Value	Source
Pilot flying (Continued)	Task Performance$_{PF}$ Goal 4: Navigation Vertical	μ_{PF}^{TW}	Duration in *Monitoring & Decision*	10 s	Expert
		μ_{PF}^{MD}	Mean duration of *Monitoring & Decision* → *Coordination*	∞	Expert
		μ_{PF}^{Coord}	Mean duration of *Coordination* → *Monitoring & Decision*	0 s	Expert
		μ_{PF}^{ExMon}	Mean duration of *Execution Monitoring* → *Monitoring & Goal Prioritisation*	20 s	Expert
		μ_{PF}^{MonGP}	Mean duration of *Monitoring & Goal Prioritisation* → *End Task*	10 s	Expert
		μ_{PF}^{Mon}	Mean duration of *Monitoring* → *Monitoring & Decision* (i.e. before evaluating a new vertical manoeuvre to leave SSA)	20 s	Expert
	Task Performance$_{PF}$ Goal 5 (Nav. Horizontal	μ_{PF}^{MD}	Mean duration of *Monitoring & Decision* → *Coordination*	∞	Expert
		μ_{PF}^{Coord}	Mean duration of *Coordination* → *Monitoring & Decision*	0 s	Expert
		μ_{PF}^{ExMon}	Mean duration of *Execution Monitoring* → *Monitoring & Goal Prioritisation*	20 s	Expert
		μ_{PF}^{MonGP}	Mean duration of *Monitoring & Goal Prioritisation* → *End Task*	10 s	Expert
		μ_{PF}^{Mon}	Mean duration of *Monitoring* → *Monitoring & Decision*	20 s	Expert

Agent	LPN	Parameter	Explanation	Value	Source
Pilot flying (Continued)	Task Performance$_{\text{PF}}$ Goal 6: Prepare Route Change	μ_{PF}^{MD}	Mean duration of *Monitoring & Decision* → *Coordination*	∞	Expert
		μ_{PF}^{Coord}	Mean duration of *Coordination* → *Monitoring & Decision*	0 s	Expert
		μ_{PF}^{ExMon}	Mean duration of *Execution Monitoring* → *Monitoring & Goal Prioritisation*	20 s	Expert
		μ_{PF}^{MonGP}	Mean duration of *Monitoring & Goal Prioritisation* → *End Task*	10 s	Expert
		μ_{PF}^{MD2E}	Mean duration of *Monitoring & Decision* → *Execution*	10 s	Expert
	Task Performance$_{\text{PF}}$ Goal 7: Miscellaneous	μ_{PF}^{MD}	Mean duration of *Monitoring & Decision* → *Coordination*	∞	Expert
		μ_{PF}^{Coord}	Mean duration of *Coordination* → *Monitoring & Decision*	0 s	Expert
		μ_{PF}^{ExMon}	Mean duration of *Execution Monitoring* → *Monitoring & Goal Prioritisation*	20 s	Expert
		μ_{PF}^{MonGP}	Mean duration of *Monitoring & Goal Prioritisation* → *End Task*	10 s	Expert
		μ_{PF}^{MD2E}	Mean duration of *Monitoring & Decision* → *Execution*	10 s	Expert
	Task Performance$_{\text{PF}}$	μ_{PF}^{Mon}	Duration parameter of *Monitoring* → *Monitoring & Decision*	20 s	Expert
		μ_{PF}^{TD}	Duration parameter of *Monitoring* → *Monitoring & Goal Prioritisation*	3 min	Model
	State Situational Awareness$_{\text{PF}}$	z_{PF}^{maxFL}	SA by PF of maximum FL	FL 440	Model
		z_{PF}^{minFL}	SA by PF of minimum FL	FL 100	Model

Agent	LPN	Parameter	Explanation	Value	Source
Pilot flying (Continued)	Intent Situational Awareness$_{\text{PF}}$	ISA$_{FL}$	Intended FL	FL 320	Model
		ISA$_{VS_{\text{Climb}}}$	Intended ROC	1500 ft/min	Expert
		ISA$_{VS_{\text{Climbx}}}$	Intended ROC expedite	2000 ft/min	Expert
		ISA$_{VS_{\text{Desc}}}$	Intended ROD	-2000 ft/min	Expert
		ISA$_{VS_{\text{Descx}}}$	Intended ROD expedite	-3000 ft/min	Expert
		FL_{SSA}	SSA minimum FL	FL90	Model
	Cognitive Mode	$m_{\text{PF}}^{\text{goals}}$	Total number of goals of PF	7	Model
		$m_{\text{PF}}^{\text{failures}}$	Total number of failures in case of 'Emergency actions' goal for PF	6	Model
		$\mu_{\text{PF},i}^{\text{opp}}$	Mean duration of *Opportunistic* mode for PF of aircraft $i = \{1 \dots n\}$	5 min	Expert
Pilot not flying	Task Perf.$_{\text{PNF}}$	μ_{PNF}^{MD}	Mean duration of *Monitoring & Decision* $\rightarrow$ *Coordination*, Mean duration of *Monitoring & Decision* $\rightarrow$ *Monitoring*	5 s	Expert
		μ_{PNF}^{Coord}	Mean duration of *Coordination* $\rightarrow$ *Monitoring & Decision*	2 s	Expert
		μ_{PNF}^{ExMon}	Mean duration of *Execution Monitoring* $\rightarrow$ *Monitoring & Goal Prioritisation*	5 s	Expert
		μ_{PNF}^{MonGP}	Mean duration of *Monitoring & Goal Prioritisation* $\rightarrow$ *End Task*	5 s	Expert
		μ_{PNF}^{Mon}	Mean duration of *Monitoring* $\rightarrow$ *Monitoring & Decision*	5 s	Expert
		$m_{\text{PF}}^{\text{failures}}$	Total number of failures in case of 'Emergency actions' goal for PF	6	Model

Agent	LPN	Parameter	Explanation	Value	Source
Global GNC system	GNSS system (Nav Global) / Satellites	$\mu_{\text{SAT}}^{\text{down}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	1/2 hr	Model
		$\mu_{\text{SAT}}^{\text{degraded}}$	Mean duration of *Degraded* $\rightarrow$ *Working*	0 s	Model
		$\mu_{\text{SAT}}^{\text{corrupted}}$	Mean duration of *Corrupted* $\rightarrow$ *Working*	1/2 hr	Model
		$p_{\text{SAT}}^{\text{down}}$	Probability of *Not Working*	10^{-5}	GNSS info
		$p_{\text{SAT}}^{\text{degraded}}$	Probability of *Degraded*	0	Model
		$p_{\text{SAT}}^{\text{corrupted}}$	Probability of *Corrupted*	10^{-20}	GNSS
	ADS-B (Global) / Ether frequency (1090) occupied	$\mu_{\text{ADS,FRQ}}^{\text{occupied}}$	Mean duration of *Occupied* $\rightarrow$ *Not occupied*	1 hr	Expert
		$p_{\text{ADS,FRQ}}^{\text{occupied}}$	Probability of *Occupied*	10^{-6}	Model
	SSR frequency (1030) occupied	$\mu_{\text{SSR,FRQ}}^{\text{occupied}}$	Mean duration of *Occupied* $\rightarrow$ *Not occupied*	0 s	model
		$p_{\text{SSR,FRQ}}^{\text{occupied}}$	Probability of *Occupied*	0	model
Airborne GNC systems	Indicators Failure Mode PF	$\mu_{\text{HMI}}^{\text{down}}$	Mean duration of *HMI not working* $\rightarrow$ *HMI working*	0 s	model
		$p_{\text{HMI}}^{\text{down}}$	Probability of *HMI not working*	0	model
		$m_{\text{PF}}^{\text{failures}}$	Total number of failures in case of 'Emergency actions' goal for PF	6	Model

Agent	LPN	Parameter	Explanation	Value	Source
Airborne GNC systems (continued)	Aircraft Guidance	$\mu^{\text{down}}_{\text{GUID}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	0 s	Expert
		$p^{\text{down}}_{\text{GUID}}$	Probability of *Not Working*	0	Expert
	Horizontal Guidance Configuration Mode	σ^{χ}_{err}	standard deviation of course error when LNAV disengaged	0.5^{o}	Expert
	Vertical Guidance Configuration Mode	$\sigma_{\epsilon_\perp}$	Standard deviation on position of aircraft entering the system, vertical direction	20 m	(CAA, 1993)
		$\sigma_{\nu_\perp}$	Standard deviation on velocity of aircraft entering the system, vertical direction	0.5 m/s	Model
		b_3	Noise factor on velocity, vertical direction	0.1 m/s	Model
		d^z_{level}	boundary value used to determine if the aircraft is flying level or climbing/descending	10 m	Model
		σ^w_z	standard deviation vertical wind	0 m/s	Model
		μ^w_z	mean vertical wind	0 m/s	Model

Agent	LPN	Parameter	Explanation	Value	Source
Airborne GNC systems (continued)	Aircraft FMS Intent	$\mu_{bank}^{Intended}$	intended bank angle	25^{o}	Expert
		$V_g^{Intended}$	intended groundspeed	250 m/s	Model
		ANP	ANP value	1 Nm	Concept
		CB_{fx}^{Hor}	factor for Horizontal Conformance boundary , i.e, boundary value (in Nm) is $0.5 \cdot ANP \cdot CB_{fx}^{Hor}$	2x	Model
		CB_{fx}^{Ver}	factor for Vertical Conformance boundary , i.e, boundary value (in m) is $\sigma_{\epsilon_\perp} \cdot CB_{fx}^{Ver}$	2x	Model
		TCP_{Time}^{Send}	duration for sending one trajectory change point (TCP)	3 s	Expert
		TCP_{Num}^{Send}	number of TCP's sent belonging to intent (hence total duration of sending intent takes $TCP_{Time}^{Send} \cdot TCP_{Num}^{Send}$)	4	Expert
		d_{const}^{Prio}	a/c priority (w.r.t. distance to Goal) is constant within this range (to avoid continuous switching of priorities)	10 Nm	Model
	Aircraft GNSS Receiver	$\mu_{\text{GNSS}}^{\text{down}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	500 s	Expert
		$p_{\text{GNSS}}^{\text{down}}$	Probability of *Not Working*	$5\ 10^{-5}$	Expert
	Aircraft IRS	$\mu_{\text{IRS}}^{\text{down}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	0 s	Expert
		$p_{\text{IRS}}^{\text{down}}$	Probability of *Not Working*	0	Expert
	Aircraft Altimeter	$\mu_{\text{ALT}}^{\text{down}}$	Mean duration of *Degraded* $\rightarrow$ *Working*	1/2 hr	Expert
		$p_{\text{ALT}}^{\text{down}}$	Probability of *Degraded*	$5\ 10^{-5}$	Expert

Agent	LPN	Parameter	Explanation	Value	Source
Airborne GNC systems (continued)	Aircraft Horizontal Position Processing	σ_x^{IRS}	Standard deviation of horizontal position error in case of IRS estimate	0 m	DADI2 EMERTA
		c_1	Covariance of horizontal position and velocity error in case of IRS estimate	0 m^2/sec	DADI2 EMERTA
		σ_v^{IRS}	Standard deviation of horizontal velocity error in case of IRS estimate	4 Nm/hr	DADI2 EMERTA
		σ_x^{GNSS}	Standard deviation of horizontal position error in case of GNSS working well	20 m	Expert
		σ_v^{GNSS}	Standard deviation of horizontal velocity error in case of GNSS working well	2 m/s	Expert
		$\sigma_x^{GNSS,DC}$	Standard deviation of horizontal position error in case of GNSS degraded or corrupted	20 m	Expert
		$\sigma_v^{GNSS,DC}$	Standard deviation of horizontal velocity error in case of GNSS degraded or corrupted	10 m/s	Expert

Agent	LPN	Parameter	Explanation	Value	Source
Airborne GNC systems (continued)	Aircraft Vertical Position Processing	σ_x^{ver}	Standard deviation of vertical position error in case of altimeter working well	10 m	Expert
		σ_v^{ver}	Standard deviation of vertical velocity error in case of altimeter working well	1 m/s	Expert
		$\sigma_x^{ver,degr}$	Standard deviation of vertical position error in case of altimeter degraded or corrupted	60 m	Expert
		$\sigma_v^{ver,degr}$	Standard deviation of vertical velocity error in case of altimeter degraded or corrupted	2 m/s	Expert
		b	Noise factor on velocity	0.5 m/s	Model
	ADS-B transmitter (1090 Mhz squitter)	$\mu^{\text{down}}_{\text{ADS,TRM}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	1/2 hr	Expert
		$p^{\text{down}}_{\text{ADS,TRM}}$	Probability of *Not Working*	$5\ 10^{-5}$	Expert
	ADS-B receiver (1090 Mhz receiver)	$\mu^{\text{down}}_{\text{ADS,REC}}$	Mean duration of *Not Working* $\rightarrow$ *Working*	1/2 hr	Expert
		$p^{\text{down}}_{\text{ADS,REC}}$	Probability of *Not Working*	$5\ 10^{-5}$	Expert
	Regular Broadcast FMS Intent	T_{IRB}	time interval for regular broadcast of intent to other ac	2 min	Model

Agent	LPN	Parameter	Explanation	Value	Source
ASAS	ASAS CD & Management	T^{x}_{update}	duration before Processing update of state info	1.5 s	Model
		T^{I}_{update}	duration before Processing update of Intent info	1.5 min	Model
		T^{STC}_{pred}	STC prediction time of potential conflict	3 min	Model
		T^{MTC}_{pred}	MTC prediction time of potential conflict	10 min	Model
		T_{SoD}	time duration after which Start of Descend (leaving SSA) will be initiated in case of Nav failure	10 s	Expert
		$H^{MTCD}_{sepASAS}$	Vertical separation used in ASAS MTCD	1000 ft	Concept
		$H^{STCD}_{sepASAS}$	Vertical separation used in ASAS STCD	900 ft	Concept
		$R^{MTCR}_{resASAS}$	Horizontal resolution distance for ASAS MTCR	5 Nm	Concept
		$H^{MTCR}_{resASAS}$	Vertical resolution distance for ASAS MTCR	1000 ft	Concept
		$R^{STCR}_{resASAS}$	Horizontal resolution distance for ASAS STCR	3 Nm	Concept
		$H^{STCR}_{resASAS}$	Vertical resolution distance for ASAS STCR	900 ft	Concept
		$\Delta\phi^{B2Goal}_{max}$	maximum turn angle allowed for flying back to goal after STCR	90^{o}	Model

Agent	LPN	Parameter	Explanation	Value	Source
ASAS (continued)	ASAS Resolution Mode	T_{res}^{STC}	duration of state-based short term conflict before ASAS "switches" to STC resolution mode	10 s	Expert
		$T_{AlertAgain}^{STC}$	if an STC conflict exists longer than $T_{AlertAgain}^{STC}$, then another alert is generated	30 s	Expert
		$T_{AlertAgain}^{MTC}$	if an MTC conflict exists longer than $T_{AlertAgain}^{MTC}$, then another alert is generated	2 min	Expert
		$\Delta\tau_{in}^{STC}$	If another STC is predicted to occur $\Delta\tau_{in}^{STC}$ earlier than the existing earliest STC, then an STC alert is generated	5 s	Expert
		$\Delta\tau_{in}^{MTC}$	If another MTC is predicted to occur $\Delta\tau_{in}^{MTC}$ earlier than the existing earliest MTC, then an MTC alert is generated	5 s	Expert

Agent	LPN	Parameter	Explanation	Value	Source
ASAS (continued)	ASAS Intent based STCR advisory	$\Delta\phi_{max}^{res}$	maximum course change for resolution	60°	Expert
		T_{add}^{STC}	additional time beyond the Short Term horizon to avoid new immediate Short Term conflicts when doing ST resolution	10 s	Model
		R_{min}^{res}	minimum reduced horizontal separation value allowed if no horizontal resolution can be found	100 m	Model
		T_{STCR}^{CPU}	time duration to calculate STCR	1 s	Expert
		$\Delta\phi_{deg}^{div}$	angle used to diverge parallel STCR's	5°	Model
		H_{Bound}^{div}	all a/c within H_{Bound}^{div} height difference are initially taken into account for divergence of parallel STCR's	300 ft	Model
		$H_{Bound}^{divStep}$	stepwise increase of H_{Bound}^{div}-value if there are no a/c within H_{Bound}^{div} height difference	100 ft	Model
		d_{ROT}^{Step}	stepsize in course change for finding short term conflict resolution	0.5°	Model

Agent	LPN	Parameter	Explanation	Value	Source
ASAS (continued)	ASAS Intent based MTCR advisory	$\Delta\phi_{max}^{res}$	maximum course change for resolution	60°	Expert
		T_{add}^{MTC}	additional time beyond the Medium Term horizon to avoid new immediate Medium Term conflicts when doing MT resolution	5 min	Expert
		T_{MTCR}^{CPU}	time duration to calculate MTCR	2 s	Expert
		$\Delta\phi_{deg}^{MTCR}$	stepsize in course for finding medium term conflict resolution	0.5°	Model
		$\Delta\phi_{B2Gmax}^{MTCR}$	maximum turn angle allowed in "back to goal" part of resolution	45°	Model
		Δd_{B2Gmax}^{MTCR}	maximum detour distance allowed for MTCR	15 Nm	Expert
		ΔT_{B2G}^{MTCR}	time interval at which a waypoint is placed to find a path "back to goal"	15 s	Model
		$\Delta\tau_{Adviz}^{MTCR}$	MTCR "starts" at $t + \Delta\tau_{Adviz}^{MTCR}$ (to take sending duration of intent to other a/c into account)	20 s	Model
	ASAS State & Intent other ac	$T_{update}^{ASAS-SI}$	duration before automatic reprocessing of Info (determine if info has become too old)	1 min	Expert
		T_{drop}^{State}	time difference for dropping State info of other aircraft (i.e. info too old)	10 s	Expert
		T_{drop}^{Intent}	time difference for dropping Intent info of other aircraft (i.e. info too old)	6 min	Model
		R^{ADS-B}	ADS-B range (horizontal)	∞	(*)

(*) It is assumed that SWIM provides an umlimited extension of ADS-B reach without causing any extra delay.

Agent	LPN	Parameter	Explanation	Value	Source
ASAS (continued)	ASAS Conf. Mon. Intent other ac	Td_{Dist}^{CMI}	time duration bound for horizontal and vertical distance conformance	2 s	Expert
		Td_{ϕ}^{CMI}	time duration bound for course conformance	2 s	Expert
		Td_{Vg}^{CMI}	time duration bound for groundspeed conformance	2 s	Expert
		Td_{Mode}^{CMI}	time duration bound for Maneuvre-mode conformance	7 s	Model
		$Td_{V\perp}^{CMI}$	time duration bound for vertical speed conformance	7 s	Model
		ϕ_{bound}^{Course}	course conformance bound	5°	Expert
		V_g^{Bound}	groundspeed conformance bound	10 m/s	Expert
		$V_{\perp,Level}^{Bound}$	vertical speed conformance bound when flying Level	0.1 m/s	Expert
		$V_{\perp,NLevel}^{Bound}$	vertical speed conformance bound when climbing/descending	2 m/s	Expert
	ASAS Surveillance other ac	T_{update}^{surv}	duration before ADS-B info update of all other aircraft	1 s	ADS-B
		u^{occ}	probability that any other aircraft j is not received by own aircraft i due to ADS-B Global Occupied or Not.	0.5	Expert

Agent	LPN	Parameter	Explanation	Value	Source
ASAS (continued)	ASAS System Mode	$\mu^{\text{fail}}_{\text{ASAS}}$	Mean duration of *Failure* $\rightarrow$ *Working*	1 hr	Model
		$\mu^{\text{corrupted}}_{\text{ASAS}}$	Mean duration of *Corrupted* $\rightarrow$ *Working*	1 hr	Model
		$p^{\text{fail}}_{\text{ASAS}}$	Probability of *Not Working*	$5\ 10^{-5}$	Expert
		$p^{\text{corrupted}}_{\text{ASAS}}$	Probability of *Corrupted*	$5\ 10^{-5}$	Expert