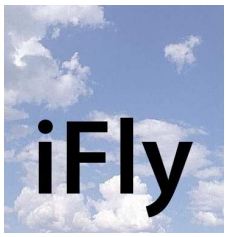

Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

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 D7.1b

Hazard Identification and Initial Hazard Analysis of A^3 ConOps based operation

Version: Draft 0.8

H.A.P. Blom, G.J. Bakker, M.B. Klompstra and F.J.L. Bussink
NLR

Due date of deliverable: 22 March 2009
Actual submission date: 31 August 2009

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:	*Hazard Identification and Initial Hazard Analysis of A³ ConOps based operation*
Authors of document:	*H.A.P. Blom, G.J. Bakker, M.B. Klompstra and F.J.L. Bussink*
Deliverable number:	*D7.1b*
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	6 March '09	All	First draft
0.2	30 April '09	All	Second draft
0.3	13 May '09	All	Third draft
0.4	7 Aug '09	All	Fourth draft
0.5	20 Aug '09	All	Fifth draft
0.6	24 Aug '09	All	Sixth draft
0.7	31 Aug '09	All	EC submitted version
0.8	11 Sep '09	Sections 3-5	Updated version

Authors	H.A.P. Blom	NLR	
	G.J. Bakker	NLR	
	M.B. Klompstra	NLR	
	F.J.L. Bussink	NLR	
Internal reviewers	J.J. Scholte	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 current report performs a first safety directed evaluation of this advanced operation. Through brainstorms with pilots and controllers potential hazards are identified. Subsequently an initial hazard analysis of these potential hazards is being conducted.

Table of Contents

Acronyms

Acronym	Definition
A^3	Autonomous Aircraft Advanced
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependant Surveillance - Broadcast
AFR	Autonomous Flight Rules
AICAS	Engine Indicating and Crew Alerting System
AMFF	Autonomous Mediterranean Free Flight
ANP	Actual navigation performance
ANSP	Air Navigation Services Provider
ASAS	Airborne Separation Assistance System
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATI	Aeronautical Telecommunication Information
ATM	Air Traffic Management
BT	Business Trajectory
CD	Conflict Detection
CD&R	Conflict Detection and Resolution
CDTI	Cockpit Display of Traffic Information
ConOps	Concept of Operations
CR	Conflict Resolution
CTA	Controlled Time of Arrival
DCB	Demand and Capacity Balancing
ECAM	Electronic Centralised Aircraft Monitoring
FFAS	Free Flight Airspace (outdated)
FMS	Flight Management System
FOC	Flight Operations Centre
FPCM	Flight Plan Conformance Monitoring
ICAO	International Civil Aircraft Association
LoS	Loss of Separation
MAS	Managed airspace
MTCR	Medium Term Conflict Resolution
NOTAM	Notice To Airmen
OSED	Operational Services and Environmental Description
P-ASAS	Predictive Airborne Separation Assurance System
R/T	Radio Telecommunications
RBT	Reference Business Trajectory
RTA	Required Time of Arrival
RTD	Research, Technology and Development
RVSM	Reduced Vertical Separation Minima
SA	Situational Awareness
SES	Single European Sky
SESAR	SES Advanced Research

Acronym	Definition
SSA	Self Separation Airspace
SSEP	Airborne Self Separation
STC	Short Term Conflict
STCR	Short Term Conflict Resolution
SWIM	System Wide Information Management
TA	Traffic Alert
TA/RA	Traffic Advisory/Resolution Advisory
TCAS	Tactical Collision Avoidance System
TMA	Terminal Area
TOPAZ	Traffic Organization and. Perturbation AnalyZer
UAV	Unmanned Air Vehicle
WP	Work Package

1 Introduction

1.1 iFly project

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 iFly project addresses these critical issues by developing a paradigm step change in advanced ATM concept development through a systematic exploitation of state-of-the-art mathematical techniques including stochastic modelling, analysis, optimisation and Monte Carlo simulation.

The iFly project will develop a highly automated ATM design for en-route traffic, which takes advantage of autonomous aircraft operation capabilities and which is aimed to manage a three to six times increase in current en-route traffic levels.

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 current air traffic levels. These innovative methods find their roots in robotics, financial mathematics and telecommunications.

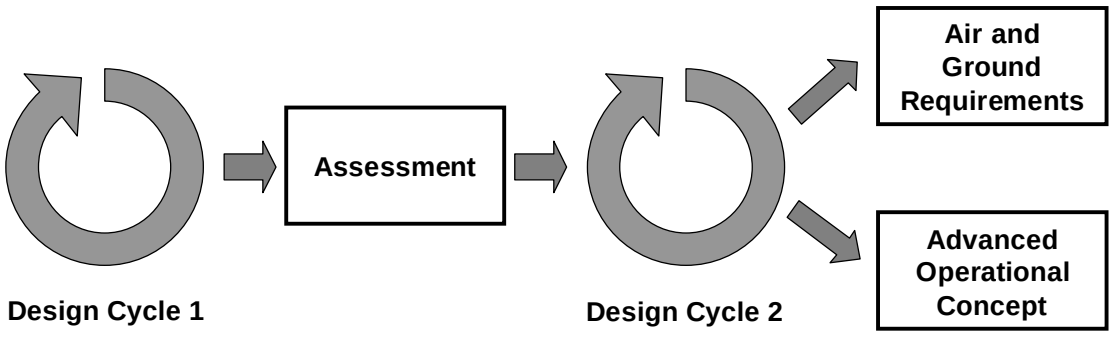

Figure 1. iFly Work Structure.

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.

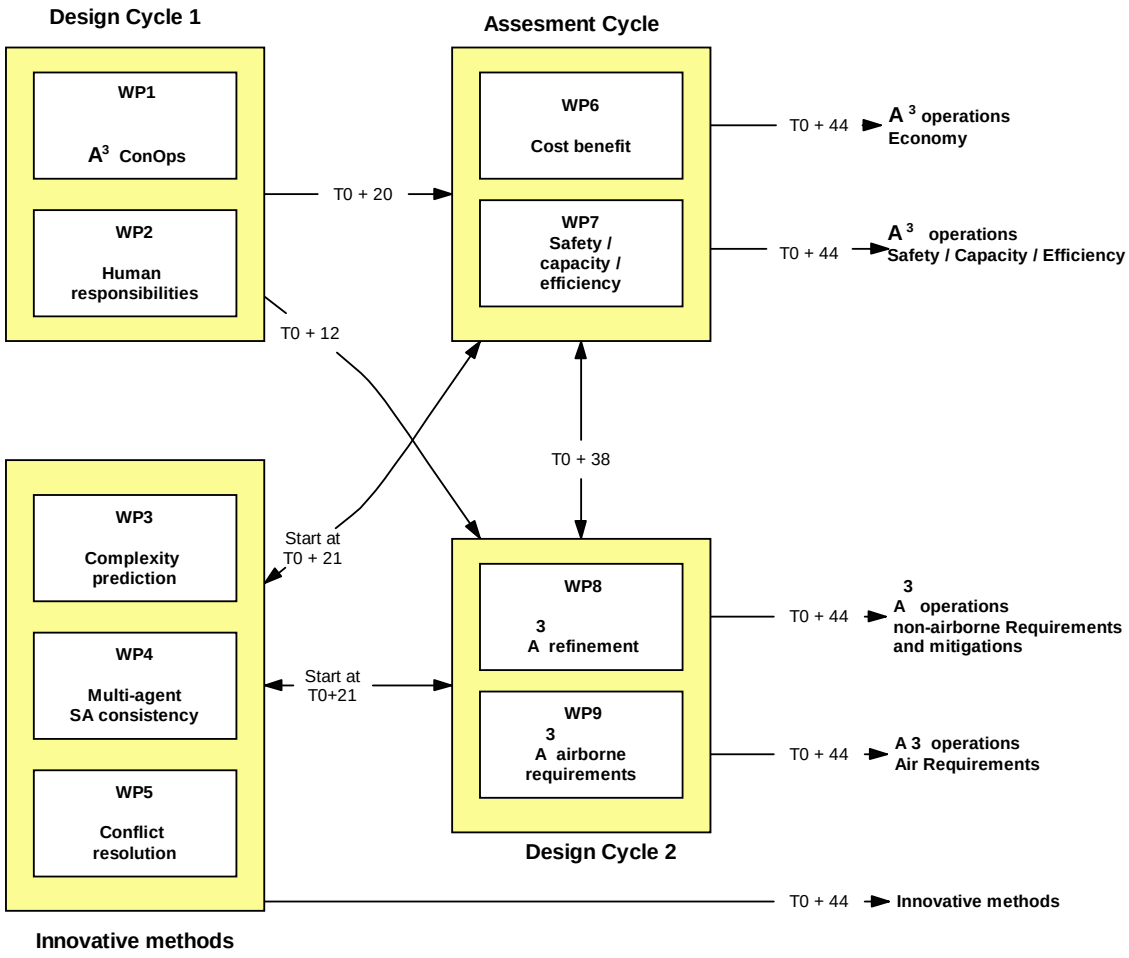

Figure 2. Organisation of iFly research.

1.2 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, and to assess the efficiency of the flights. The accident risk levels assessed should be in the form of an expected value, a 95% uncertainty area, and a decomposition of the risk level over the main risk contributing sources. The latter verifies which of these sources should be mitigated during the 2nd design cycle. 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 four sub-WPs:

- WP7.1: Monte Carlo simulation model of A^3 operation
- WP7.2: Monte Carlo speed up methods
- WP7.3: Perform Monte Carlo simulations
- WP7.4: Final report

The current D7.1b report makes part of WP7.1.

1.3 WP7.1 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 to be 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 ICAO and ESARR4 regulation. This has been reported in iFly deliverable D7.1a on 'Scoping and safety target' [iFly D7.1a]. Then, a hazard identification and initial hazard analysis is performed for the A^3 operation as has been developed by WP1 and WP2 [iFly D1.3, iFly D2.2], which is the subject of the current D7.1b report.

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 will be reported in iFly deliverable D7.1c.

1.4 Purpose and organisation of this report

The current report performs a first safety directed evaluation of this advanced operation. Through brainstorms with pilots and controllers potential hazards are identified. Subsequently an initial hazard analysis of these potential hazards is being conducted. This study has a dual purpose. The first purpose is to gain insight in the type of scenarios that should be considered in the sequel of the safety analysis, i.e. in WP7.3. The second purpose is that the initial hazard analysis results place the A^3 ConOps into a new perspective regarding safety. For any advanced concept design, it is important to become aware of the weakest links in the chain. This subsequently allows the designers to learn from this and subsequently improve their A^3

ConOps design for these weakest links. Hence the expectation is that WP4, WP8 and WP9 can use the result of this initial hazard analysis in order to further improve the A^3 ConOps. More specifically, for WP4 this is expected to identify which specific multi-agent situation awareness conditions deserve most attention. For WP9 this is expected to be of use in the derivation of safety requirements. And for WP8 this is expected to be of use for the further refinement of the A^3 ConOps, and for the development of a vision how A^3 ConOps fits best within SESAR.

This report is organised as follows. Section 2 introduces the A^3 operation considered. Section 3 identifies hazards through scenario directed brainstorms with pilots and air traffic controllers. Section 4 performs an initial hazard analysis. Section 5 provides concluding remarks.

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 et al., 2009] refers to this ConOps as Autonomous Mediterranean Free Flight (AMFF) and shows that this AMFF 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 as many conflicts as it solves. 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. This concept also allows mixed airborne equipment in the sense that non-equipped aircraft are assumed to be supported by air traffic control. The iFly A^3 ConOps developed in [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 (so-called 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 starts out some 5 to 20 minutes prior to potential loss of separation (LoS). 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 Short Term Conflict Resolution (STCR). STCR starts some 5 minutes ahead of potential loss of minimum separation (LoS). When such an event is detected, then no priority exists and all aircraft involved have to manoeuvre The applied manoeuvres shall be coordinated through so-called implicit coordination. Implicit coordination 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.

3 Potential hazard identification

The aim of this section is to identify hazards that potentially lead to (non-nominal) conditions which affect the effectiveness of the Medium Term Conflict Resolution (MTCR). First, Subsection 3.1 describes the preparation of a hazard identification brainstorm workshop that was dedicated to the A^3 ConOps. Next, Subsection 3.2 describes the outcomes of this A^3 dedicated brainstorm. Subsequently, Subsection 3.3 explains the way we have identified a set of hazards from an earlier study, most of which also seem to be of interest for the current study.

3.1 Preparation of the brainstorm participants

On the 30th of May 2008 a Hazard brainstorm meeting has been held in the Tallinn site of the University of Tartu [Klompstra, 2008b]. The aim of the brainstorm session was to perform a potential hazard identification for the A^3 ConOps [iFly D1.3] through active involvement of operational experts (three pilots and one air traffic controller). Because the A^3 ConOps based airborne self separation operation differs a lot from current practice, these participants first had to familiarize themselves with the A^3 ConOps and its implications to their way of working. One of the co-authors of [iFly D1.3] gave a presentation of the A^3 ConOps. Subsequently the brainstorm participants had ample opportunity to ask questions and to receive further explanations.

Next, the A^3 ConOps was discussed between the operational experts. During this discussion several views have been expressed, which provide an insight into the challenges pilots and controllers are facing in building a proper understanding of such an advanced concept in a short period of time:

- The initial assumption was that pilots would have been trained for one year, they would know the system and trust the system, but they might have a lingering distrust from when the system was first introduced. One of the pilots remarked that he would distrust the system anyway, even if the proposed conflict resolution manoeuvre would have been calculated correctly.
- Another pilot adds to this that a similar trust/distrust issue also exists today. The pilot is always responsible for the safety of the flight; and this creates a sensitive balance between the trust in a controller versus own judgement or responsibilities. For this reason a pilot does not like to solely rely on the controller, but rather wants to be able to backup controller decisions with some airborne electronic means. A lack of such means force a pilot to completely trust the controller's decision. While this may be the case the pilot will always re-assess this decision.
- An historical example is the introduction of ACAS (ACAS is the official ICAO term for Honeywell's TCAS). At the time, the pilot's community was pleased that TCAS would be introduced as it enabled them to see what colleagues were doing. With that capability pilots started to act like airborne controllers. This improper use of the system caused a misconception in the pilot's community. Pilots felt that TCAS would interfere with ATC. Nowadays TCAS is accepted, but it took 10 years to get used to it and use it correctly.
- One pilot remarked that certain ATC commands may not always the best option from a military pilot point of view. As an illustration he stated: "I was once in a pretty dense area, the controller directed me for a holding, however I was aware that by complying

with the controllers, I would enter a prohibited area.". Because of his Situational Awareness (SA) the pilot tried to interfere but did not get any chance to either reject the ATC call or get the message to the controller because of com saturation on that frequency. Human interaction was not possible. One pilot commented: "In the A^3 concept we leave issues like these up to electronic gadgets. As I consider one of the ATC function to be the overall mission commander in charge. Who's going to take that chair? Similar concern have also been raised with the introduction of Reduced Vertical Separation Minima (RVSM)".

- In a 3D ATC environment there are many ways to solve a separation problem therefore controllers will always look for the best solution. However, it was remarked that humans stick to their habits, as a result of which machines (systems) may be better capable to do this. For the en-route phase of the flight, one controller remarked that he is more of a manager, and does not want to control separation.
- A controller has a maximum capacity limit he is able to cope with. This is reflected for instance in the fact that controllers can't have more than a certain amount of aircraft (e.g. 20) in their sector. At the same time, a pilot too has a capacity limit and furthermore he/she may not be able to obtain a global understanding of the situation.
- In the current system pilots tend to trust controllers, as trust 'is a vital part of the system'. However this trust may not always exist everywhere. An example of this is the language problem in Chicago O'Hare, a busy airport, where the controllers speak American (which is not an official R/T language) and where there is no time to confirm the ATCo commands. "You must be extremely aware of this when approaching Chicago." In other parts of the world there may, besides a language problem also be controller capability and training problems. Crews usually try to "circumnavigate" these situations by for instance not accepting certain radar vectors. In these environments there is a *confidence* issue.
- A benefit of the current system is that pilots can hear how relaxed or stressed a controller is.
- One of the Pilots commented that "In a cockpit you always know what support you need from ATC." The ATCo adds to this: "Under emergency, ATC does not interfere and imposes silence to allow the crew to solve the situation onboard, except for those cases where assistance is requested. In these cases ATC is just a means for aircraft to transfer or provide information."
- A comparison was made with a telephone switchboard. In the old days there was human interaction, nowadays there is none. One pilot expressed his worries about the A^3 concept: "What if I get into a situation where I can't speak to a controller, there are cases where I will miss contact with a human."
- One of the concept designers explained that communication capabilities will be available in the form of air to air surveillance and data-communication. In normal operations there will always be a possibility for direct pilot-pilot communication – through radio (there is an open frequency for each sector).
- One pilot wondered: "What could be a course of action if a plane is highjacked while in conflict and the crew can't react to the resolutions given by the system?" The concept developers explained that if the high-jacked aircraft would be able to announce its situation, priority will go towards the high-jacked aircraft and all other aircraft will have to resolve any conflicts. If the situation is not know, conflicts will be solved by other aircraft when priority drops as result of the Short Term timeframe in which all aircraft have to manoeuvre.
- One of the pilots stated that he does not foresee any major problems with the future A^3 environment: "You will get some inputs and you will react, for which there will be a

checklist. What matters is that you have been trained for that environment, and how much you have been working with it."

- The ATCo adds to this, that the question really is why we need ATC? Generally speaking - for separation, information and alerting? ATC does not fly the aircraft, it is there to provide service. TCAS has already proved itself and future technologies allow implementing automated services (e.g. SWIM) so it is a natural evolution that the role of ATC is changing to monitoring, and this makes self separation a logical development. It should however be noticed that in the A^3 ConOps intentionally (and hypothetically) there is no ATC at all to monitor en route air traffic.

3.2 Hazard identification brainstorm sessions

For the potential hazard identification, three sessions have been conducted:

- ***Session I:*** Short initial brainstorm. The scope of this brainstorm was cruise level only (i.e. en-route without any climbing or descending flight phases).
- ***Session II:*** During this session a scenario guided brainstorm was conducted. The scenario considered consisted of aircraft having initial flightplans, which are in the same or opposite direction (i.e., multiple aircraft from A to B and from B to A, there is no crossing traffic). Again, the scope of this brainstorm was cruise level only.
- ***Session III***: During this session another scenario guided brainstorm was conducted. The two scenarios considered consist of crossing initial flightplans (i.e. opposite flying aircraft streams and crossing aircraft streams). Again the scope of this brainstorm was cruise level only.

The brainstorm participants were well informed that during a brainstorm session it is not allowed to analyse or to discuss the validity or relevance of any potential hazard. Even potential hazards which later on may turn out not to be real hazards may play a crucial role in the healthy evolution of the brainstorm. And such hazards even may later on turn out to be of value for the safety analysts in learning to understand the specifics of the A^3 ConOps design during the true analysis of a potential hazard which then turns out not to be a true hazard. The outcomes of these sessions have been documented in [Klompstra, 2008b].

Session I results

- Pilot does not want too much information. If all data is presented, the pilot's display may be cluttered. There is a need to de-select certain information, to make the conflict visible. Otherwise pilot has no way to the heart of the conflict. If a conflict occurs, then an auto pop-up may be helpful. [Hazard T1]
- It is company dependent if a flight is operated by a single pilot or by a PF and a PNF. In the latter case there may be SA differences between PF and PNF [Hazard T2]. For the brainstorm, reference is made to the crew, without further discussing single pilot or PF and PNF.
- In the ConOps design the implementation issues are described in general, it is not stated how it is done, nor how it must be implemented. For example for the alerting system and that presentation of an alert, it is only specified that it is necessary, it is not specified where it should be presented.
- Within NASA, initial alerting data is displayed both on the Navigation display and on the ECAM system (Electronic Centralised Aircraft Monitoring) of Airbus and the EICAS

system (Engine Indicating and Crew Alerting System) of Boeing. Pilot is alerted both aurally and by means of textual information.
- A situation in which proper information is provided to the pilot, but the pilot is unaware of the fact he/she is required to take action. Pilot is sitting and waiting for information without action. [Hazard T3]
- Developer's remark regarding pilot feedback on the Conflict Detection & Resolution: The system takes into account pilots preferences, and the system proposes a solution. It is possible to reject a solution, then the system recalculates other options, and takes the rejection into account (the number of proposals is not determined). Pilot preferences are also considered.
- There may only be vertical and horizontal manoeuvres available when optimizing the flight in the system (not speed manoeuvres). [Hazard T4]. Pilot questions what to do upon noticing a conflict that is far away in time. In that case it would be helpful to apply this speed change as intervention strategy. Don't we throw this away?

Session II results

- A European scenario (i.e. at the edges of the area) was considered, flying from the Canaries entering southern Spain. In the Canaries sector there is no radar coverage (lasts approximately 1 hour), so the airplane would transition from procedural airspace to Self Separating airspace.
- AFR rules state that while you can create medium term conflicts, you cannot create short-term conflicts. If boxed in, you are allowed to modify the trajectory beyond the short-term timeframe.
- Area avoidance using the Reference Business Trajectories utilizes the information received through SWIM – however this information may be wrong or incomplete, or there may be a reason for the pilot to deviate from the information, e.g. to avoid clouds for passenger comfort. As a result there may be two hazards (1) Meteo info received through SWIM is not always correct [Hazard T5]; and (2) Pilots might want to avoid more than what SWIM indicates [Hazard T6].
- Pilot's quote: "Fighter aircraft in combat training in a sector close to mine, might not be on my CDTI and can generate a problem for me." [Hazard T7]
- Passenger comfort of RTA [Hazard T8]. Explanation by one of the pilots: If the arrival time is fixed and inflexible, then each knot change in wind may need a change in airspeed, which may lead to discomfort to the passengers.
- Unknown aircraft such as weather-, leasure balloons [Hazard T9]
- Aircraft with priority as a result of non-normal circumstances are in the neighbourhood [Hazard T10]. In relation to this, the following question has been raised: Would it be helpful to know priority levels of surrounding aircraft? The answer provided by the A^3 ConOps designers was: Yes each aircraft broadcasts its priority level.
- UAV in neighbourhood [Hazard T11]
- Non-proper A^3 ConOps equipped aircraft in SSA [Hazard T12]
- Global weather change implies changes for multiple aircraft [Hazard T13]
- Rules of the air (unclear, misunderstood), i.e. rules how to deal with conflicts by ASAS avionics might conflict with the basic rules of 'Rules of the Air' [Hazard T14]
- Highjack or uncontrolled aircraft [Hazard T15]
- Pilots sleeping [Hazard T16]
- SWIM bandwidth issues and lack of back-up in SWIM [Hazard T17]

- Awareness confusion because of too much information [Hazard T18]. Example: pilot flies into mountain while not aware due to too many layers of information in CDTI: weather, traffic and terrain.
- Multiple military aircraft en-route-formation (Standard- vs. non-standard formation) with leader squawking only [Hazard T19]
- Positioning error (various reasons) [Hazard T20]
- The situation in which the system requires additional action from the pilot to inform SWIM of an emergency situation may lead to workload saturation at a moment that the crew is busy (this is particularly an issue in single pilot aircraft, e.g., military, general aviation, and particularly the new civilian jets coming on line) [Hazard T21]
- Flexibility will be inherent to the system. In case of an emergency, the pilot will alter the transponder code, radio communication will be open, and data communication will be available to SWIM. The emergency will be announced to other nearby aircraft. If required the pilot will have to choose another destination airport. At the same time the aircraft will get the highest priority level and possibly a modified separation classification which will free an area around the aircraft. The pilot can then select any trajectory changes in FMS, Mode Control Panel, or fly manually [Hazard T22]
- Pilot deviates from the assumed RBT [Hazard T23]. Comment from developers: Any changes to the aircraft trajectory will result in a real-time RBT update (the pilot is adjusting the RBT 'as he goes along')

Session III results

- If the trajectory management box fails there are short-term conflicts. We cannot communicate BT to everybody. Trajectory management box fails [Hazard T24]
- Envelope for trajectory management. Envelope of RBT [Hazard T25]
- Airspace may be closed totally (e.g. 9-11). (National) events of closed airspace [Hazard 26]
- Volcanic eruption resulting into closed airspace (was not predicted). Volcanic eruption [Hazard T27]
- Pilot can disconnect FMS and fly himself [Hazard T28]
- Pilot disconnects FMS [Hazard T29]
- State vector may not be useable to predict conflict [Hazard T30]. Comment: This exactly is the reason that the A^3 ConOps proposes to exchange intents and to use this in conflict resolution.
- If there is a serious electronical problem how can the system cope? Lightning strike, fire, smoke may form a common cause for multiple systems going down [Hazard T31]
- As a result of inertia the turn vector can be disturbed – vector goes to conflict, aircraft does not.
- An electronic NOTAM may result in a hazard if it is not shared with SWIM. The latest electronic NOTAM changes may get delayed into SWIM (E.g. special use in airspace) [Hazard T32]
- Structural design limits of the airplane, like speed range, buffeting etc. [Hazard T33]
- Special use airspace that is not static and which can not be made available to SWIM (e.g. location of the Royal family) [Hazard T34]
- Performance limitations [Hazard T35]
- Aircraft damage, e.g., birdstike damaging wings or windscreen crack of which the onboard system is not aware [Hazard T36]
- Weight uncertainty [Hazard T37]

- Performance degradation over time [Hazard T38]
- Coffin's corner [Hazard T39] being the altitude at which the margin between buffeting speed (too high a speed) and stall speed (too low a speed) is very small. Aircraft is therefore very limited in its speed envelope. 'Coffin corner' refers to an altitude limit for safe operation.
- Icing on the wings [Hazard T40]
- Different areas in the world use different unit systems; for example meter versus feet [Hazard T41]
- Inability to assess the track of other traffic [Hazard T42]. Comment: This has a relation to building confidence in the separation.
- TCAS and CDTI moves with you. Pilot's Situational Awareness is different from controller's SA as CDTI moves with the pilot. That is why TCAS is not usable for lateral manoeuvres [Hazard T43].
- TCAS/CDTI is unstable [Hazard T44]. Comment: This is a known issue, sometimes leading to jumping behaviour of other aircraft on TCAS / CDTI, and its effect on the fused traffic picture for future applications.
- Quality of position fusion results [Hazard T45]. Same comment as above.
- Quality of weather data [Hazard T46]
- Individual differences in pilots perception and behaviour (all) [Hazard T47]; 'my world may be different from his world'
- The sequence in which action is taken varies from person to person [Hazard T48]
- Airlines cultural differences [Hazard T49]
- Areas to be avoided due to icing [Hazard T50]
- Contingency management remains to be defined [Hazard T51]
- Reliability of pitot–static system [Hazard T52]
- Reliability of onboard sensors [Hazard T53]
- The use of anti-icing systems influence performance [Hazard T54]
- GPS failure affects present position and ground speed which is used by the autopilot and the FMS [Hazard T55]
- Failure reports get not through to the airline [Hazard T56]
- Spatial disorientation [Hazard T57]. Comment: See also ACAS II Safety Bulletin N7 from Eurocontrol[1].
- Loss of being ahead of events [Hazard T58]
- Failure reporting is more complex (might require more recording systems in the aircraft) [Hazard T59]

The potential hazards that have been identified during the three brainstorm sessions have been collected in Table 1.

Table 1. Potential hazards identified in Tallinn

T1	Too much information on CDTI
T2	Situational awareness differences between crew members
T3	Pilot should take action but is unaware and waiting for information
T4	For Short Term Conflict (STC) only vertical and/or horizontal manoeuvre may be useful.
T5	Weather may deviate from prediction received through SWIM

[1] See http://www.eurocontrol.int/msa/gallery/content/public/documents/ACAS_Bulletin_7_Mar-06.pdf

T6	Pilot perception of weather areas may differ from info received
T7	Indivual fighter aircraft out of a flight may be invisible
T8	Passenger comfort of RTA
T9	Unknown aircraft (e.g. weather-, leasure balloons)
T10	Aircraft with priority as a result of non-normal circumstances are in the neighbourhood
T11	UAV in neighbourhood
T12	Non-proper A^3 ConOps equipped aircraft in SSA
T13	Global weather change, which implies weather changes for multiple aircraft
T14	Rules of the air (unclear, misunderstood)
T15	Highjack or uncontrolled aircraft
T16	Pilots sleeping
T17	SWIM bandwidth issues and lack of back-up in SWIM
T18	Awareness confusion because of too much info / (autopop up)
T19	Multiple military aircraft en-route-formation (Standard- vs. non-standard formation) with leader squawking only
T20	Positioning error (various reasons)
T21	Emergency situations may lead to workload saturation at a moment that the crew is busy
T22	Pilot can put input into FMS what they like
T23	Pilot deviates from the assumed RBT
T24	Trajectory management box fails
T25	Out of envelope of RBT
T26	(National) events of closed airspace
T27	Volcanic eruption
T28	Pilot can disconnect FMS and fly himself
T29	Pilot disconnects FMS
T30	State vector may not be useable to predict conflict
T31	Common cause for multiple systems going down
T32	NOTAM changes get delayed into SWIM (Eg special use in airspace)
T33	Structural design limits of airplane (e.g. speed range, buffeting)
T34	Special use airspace that moves and which is not allowed to be entered into SWIM (e.g. Royal family)
T35	Performance limitations (e.g. heavier than aircraft system)
T36	Aircraft in-flight damage
T37	Weight uncertainty
T38	Performance degradation over time
T39	Coffin corner
T40	Icing
T41	Meter versus feet
T42	Inability to assess the track of other traffic
T43	TCAS not useable for lateral maneuvers
T44	TCAS/CDTI is unstable
T45	Quality of position fusion results
T46	Quality of weather
T47	Individual differences of pilots
T48	Sequence of actions varies
T49	Airlines cultural differences
T50	Areas to be avoided due to icing
T51	Contingency management remains to be defined
T52	Reliability of pitot-static

T53	Reliability of sensors
T54	System requirements of anti-icing systems influence performance
T55	GPS failure affects present position / ground speed used by autopilot / FMS
T56	Failure reports get not through in airline
T57	Spatial disorientation
T58	Loss of being ahead of events.
T59	Failure reporting is more complex (might require more recording systems in the aircraft)

3.3 Complementary hazard identification

In some previous studies a few less advanced airborne self separation concepts have been assessed on safety using the TOPAZ approach. Each such study included scenario directed hazard identification brainstorms with pilots and controllers. The potential hazards identified during these previous studies are available in the hazard data base of TOPAZ. Table 2 shows the relevant airborne self separation project reports for which potential hazards are available in the TOPAZ data base. From these sources, we select the most suitable set for re-use within this initial hazard analysis study.

Table 2. Potential relevant hazards available within TOPAZ hazard data base

Source	**Author, Year, Title**	**# of hazards**
[Daams, 2007]	Daams, 1997, Free Flight Hazard Identification brainstorm session	60
[Everdij, 2001]	Everdij, 2001, Minutes CARE-ASAS Activity 3 WP3.1 hazard brainstorm	55
[Klein Obbink, 2002]	Klein Obbink, 2002, MFF Self Separation Assurance OHA	34
[MFF, 2004]	MFF, 2004, Hazards identified during the Amsterdam February 2004 MFF experiments	80

The first two sources in Table 2 consider airborne self separation concepts in which aircraft are required to fly prescribed routes. The other two documents consider airborne self separation concepts without a fixed route structure. The third document is directed to potential hazards related to conflict resolution using tactical manoeuvres. The fourth document in particular identified strange potential hazards that have been obtained through brainstorms with pilots who have first been flying within the NLR developed simulated airborne self-separation environment of MFF. This makes this fourth source of identified hazards of complementary interest for the initial hazard identification and analysis in this report. Table 3 lists the 80 strange potential hazards identified within MFF project. Some of these potential hazards may be too MFF specific and therefore not applicable to the A^3 ConOps, or have to be interpreted in the context of the A^3 ConOps.

Table 3. Potential hazards identified in MFF 2004

M1	Pilots making own judgement on relevance of conflicts and acting only on conflicts judged relevant; misjudgement may lead to not reacting to an important alert.
M2	Pilots making own judgement on relevance of (reported, alerted) failures and acting only on

	failures judged relevant; misjudgement may lead to not reacting to an important alert.
M3	If situation is judged safe, no further action is taken though ASAS or ACAS still speaks of conflict.
M4	Nuisance alerts enhance the effect that pilots make own judgements of conflicts.
M5	Nuisance alert: An aircraft climbing and an aircraft descending to each other, but levelling off 10 FL before meeting. In case of intent-less ASAS this causes an alert.
M6	Nuisance alerts may be expected near the transitions between MAS and FFAS, due to the sizes of the protected areas.
M7	Nuisance alert: aircraft flying level on FL 370, another aircraft climbing to FL 380 and levelling of too slowly to prevent conflict.
M8	'Irritating P-ASAS bands' decrease the confidence in ASAS, and enhance the effect of nuisance alerts.
M9	P-ASAS bands and alerts caused by small vertical speeds in turns can be regarded as 'nuisance'.
M10	P-ASAS bands and alerts caused by small vertical speeds in turbulence can be regarded as 'nuisance'.
M11	ACAS/ASAS inconsistencies decrease confidence in ASAS, enhancing the probability that pilots overrule ASAS solutions or ACAS advisories.
M12	ACAS/ASAS inconsistencies: ACAS TAs occurring while no ASAS conflict is detected.
M13	ACAS/ASAS dependencies may cause that in case of one failure a conflict is not detected by either of them (depending on final implementation).
M14	Presented ASAS solution may bring pilot to overrule ACAS advisory (TA/RA) (depending on final implementation).
M15	Suppression of ASAS solutions in case of ACAS advisory (TA/RA) may lead to sudden loss of situational awareness of pilots (depending on final implementation).
M16	In case of an erroneous but long lasting ACAS advisory (TA/RA), suppression of ASAS Conflict Detection and Resolution may lead to the situation where both separation assurance and conflict avoidance are corrupted.
M17	If ACAS and ASAS are fed by one power bus, a failure could lead to a loss of both
M18	Decreased confidence in ASAS caused by TCAS alerts 'out of the blue' in case of navigation failures.
M19	Creative pilots managing to create their own priority. This can lead to situations in which aircraft follow unexpected routes or go all into one direction.
M20	Pilots misusing the priority status by choosing crowded parts of airspace, or by bothering a different aircraft.
M21	Crew self inflicting a failure (e.g., pulling circuit breaker) to be allowed to switch on the priority switch.
M22	In an emergency procedure, switching on the priority switch may be done late or it may be forgotten, especially in case of serious emergencies such as a rapid de-compression
M23	In an emergency procedure, aircraft may have to descend quickly and not have time to look out for other traffic.
M24	The crew may also switch on the priority switch while it should not, because of mixing up emergency procedures.
M25	If the crew thinks to have switched on the priority switch, while they still have not, they expect other aircraft to solve the conflict, while the other aircraft do not even see the conflict yet.
M26	Traffic overtaking from behind, especially when having priority, causing a conflict while they can still not be seen on the CDTI.
M27	CDTI set up such that a conflicting aircraft cannot be seen on the CDTI.
M28	Some aircraft symbols may not be seen well in sunlight, e.g., dark grey symbols.
M29	A workload that is too low.
M30	Suddenly having to switch from a very low workload to a high workload may cause ?
M31	Switching ASAS off (accidentally, or on purpose e.g. to see if it helps to get it working again

	later on).
M32	Switching ASAS in the wrong mode.
M33	Typing in a wrong separation distance (mistyping, confusing separation distance for another airspace).
M34	Typing in a wrong look-ahead time (mistyping, confusing separation distance for another airspace).
M35	Forgetting to switch on ASAS when entering FFAS.
M36	Switching ASAS in the wrong mode when entering FFAS.
M37	Switching ASAS on and off to reset the system or to recover from a failure. Crew may be interrupted by something else and continue with ASAS switched off.
M38	Fuel problems may be caused by descending into MAS.
M39	Circumventing poor weather and Special Use Airspaces causes more fuel usage.
M40	R/T position reports (after e.g. ADS-B transmission failure) can be unclear, be misunderstood or be imprecise.
M41	Position reports can be given on the wrong R/T frequency, e.g. ATI instead of the one for the airspace users.
M42	Multiple aircraft flying around in FFAS having a failure.
M43	Crew not being informed about failures of other aircraft when entering FFAS.
M44	Crews deciding not to leave FFAS when a failure occurs.
M45	Flight control related errors occur, possibly in combination with transponder problems. Especially smoke or rapid decompression.
M46	A crew not realising to have to solve a conflict after an own ADS-B transmitter failure, because they think to have priority since priority is indicated on the CDTI.
M47	A crew switching priority after an own ADS-B transmitter failure (mistakenly thinking that this might help), and then assuming that they can take right of way.
M48	Lack of a buffer area between FFAS and Special Use Airspace.
M49	Autopilot turning over (‘over steer’).
M50	Conflicts popping up when already being in a next phase. For instance, when turning into a conflict, the conflict may already be very nearby.
M51	Bands closing in from both sides, such that you cannot turn left nor right.
M52	Bands closing in from all sides, such that you cannot turn left nor right, and neither climb nor descend.
M53	Taking too much time to give a ‘distress’ call, because of unfamiliarity with the emergency procedure or the system.
M54	Within a conflict, the aircraft without priority switches on the priority button. By delays (priority update) or reduced vigilance, conflict resolution is not taken care of.
M55	Crews always giving way and solving and preventing conflicts may cause the aircraft to use much fuel.
M56	Crews always giving way and solving and preventing conflicts may cause an unstable traffic pattern.
M57	Crews turning through an amber band.
M58	The pilot forgets to tell the controller of MAS about a failure when leaving FFAS.
M59	The pilot forgets to tell the controller of FFAS about a failure when entering FFAS.
M60	Ambiguously written emergency procedures, leading to incorrect or late crew actions.
M61	Difficult emergency procedures, leading to incorrect or late crew actions.
M62	Pilots having a poor awareness of free flight logic (various examples; none particularly relevant).
M63	A navigation map shift.
M64	Priority determination based on FLOS leads to ambiguities at North and South Pole.
M65	The relevance of an emergency message is missed as callsigns are not indicated on CDTI, and the actually nearby aircraft is assumed to be far away.
M66	Cluttered display by inappropriate range setting.

M67	Two or more aircraft with priority switched on in same airspace.
M68	Disagreement between crew members on how to solve conflict.
M69	Misinterpreting or disregarding ASAS horizontal conflict solution manoeuvre by heading/track confusion.
M70	Pilots distrust ASAS information, wonder whether ASAS works fine, and, in order to check it, make some manoeuvres with the purpose to generate a potential conflict.
M71	ANP value is calculated conservatively. Common cause for all aircraft.
M72	Failure to engage NAV after flying heading
M73	GPS jamming by radio pirates
M74	Interference of ADS-B by radio pirates
M75	Interference of ADS-B is getting worse
M76	No crew
M77	Routing across military airspace
M78	TCAS interference by radio pirates
M79	Volume of alerts is turned down on headset/speakers
M80	Volume of R/T is turned down on headset/speakers

4 Initial Hazard Analysis

In comparison to earlier hazard analysis studies for airborne self separation operations, this is the first one that considers a concept in which intent information of aircraft is explicitly exchanged in order to allow each aircraft to plan and broadcast conflict free trajectories. For this reason, the initial hazard analysis in this report intentionally focuses on potential hazards that may occur during the planning and exchange of intent information. Our analysis is done through conducting a sequence of steps. The first step is to identify for each of the 59 Tallinn hazards and 80 MFF hazards (139 in total) which intent related (non-nominal) conditions are relevant (Subsection 4.1). The second step is to identify which combinations of non-nominal intent related conditions have been identified (Subsection 4.2). The third step is to evaluate the A^3 ConOps consequences for the various combinations of (non-nominal) intent related conditions, and how often these conditions and consequences are expected to happen (Subsection 4.3).

4.1 Intent related (non-nominal) conditions

First, a number of relevant (non-nominal) intent related conditions relative to an ownship aircraft perspective have been defined in Table 4 below. Subsequently, each individual hazard in Tables 1 and 3 is evaluated in order to identify which (combinations) of these non-nominal conditions apply. For the Tallinn identified potential hazards this is done in Table 5a, and for the MFF identified potential hazards this is done in Table 5b.

Table 4. Intent related (non-nominal) conditions relative to an ownship perspective

A. Broadcasted intent of ownship aircraft • A0: Everything is nominal • A1: Intent not conflict free with other aircraft • A2: Intent not viable (not flyable or unsafe) • A3: Autopilot setpoint only • A4: Not broadcasted /received
B. Received intent from other aircraft • B0: Everything is nominal • B1: Intent not conflict free for one • B1': Intent not conflict free for multiple • B2: Intent not viable for one • B2': Intent not viable for multiple • B3: Autopilot setpoint only for one • B3': Autopilot setpoint only for multiple • B4: Not received for one • B4': Not received for multiple
E. Broadcasted emergency of ownship aircraft • E0: No emergency • E1: Emergency broadcasted • E2: Fake emergency broadcasted • E3: Emergency not broadcasted

F. Received emergency from other aircraft • F0: No emergency • F1: Emergency from another aircraft received • F2: Fake emergency from another aircraft received • F3: Emergency from another aircraft not received
P. Situation Awareness (SA) of pilot(s) of the ownship aircraft: • P0: SA is fine • P1: SA differs for their own aircraft • P2: SA differs for one other aircraft • P3: SA differs for own and one other aircraft • P4: SA differs for multiple other aircraft • P5: SA differs for own and multiple other aircraft
Q. SA of pilot(s) of multiple (directly or indirectly) involved aircraft • Q0: SA is fine • Q1: SA differs for their own aircraft • Q2: SA differs for one other aircraft • Q3: SA differs for own and one other aircraft • Q4: SA differs for multiple other aircraft • Q5: SA which differs for own and multiple other aircraft
R. SA of pilot(s) of one (of the) directly involved aircraft • R0: SA is fine • R1: SA differs for their aircraft • R2: SA differs for one other aircraft • R3: SA differs for their and one other aircraft • R4: SA differs for multiple other aircraft • R5: SA differs for their and multiple other aircraft

In order to understand Tables 5a and 5b, we first explain in words how these tables should be read. For this we consider the classifications for Tallinn identified hazards 7 and 10 in Table 5a.

Tallinn identified hazard number 7 reads: “Individual fighter aircraft out of a flight may be invisible”. This is judged to lead to the following combination of non-nominal conditions: $(B4 \cap P2 \cap Q2)$, which is short for each of the following sub-conditions to apply:

- B4: Intent is not received from one other aircraft;
- P2: Pilot(s) of the ownship aircraft have an SA which differs for this other aircraft;
- Q2: Pilot(s) of multiple other aircraft also have an SA which differs for this other aircraft.

Tallinn identified hazard number 10 reads “Aircraft with priority as a result of non-normal circumstances are in the neighbourhood”. This is judged to lead to the following two possible combinations of non-nominal conditions: $(E1 \cap R2)$ or $(F1 \cap P2)$.
Here, $(E1 \cap R2)$ is short for each of the following sub-conditions to apply:

- E1: Emergency is broadcasted by Ownship
- R2: Pilot(s) of another aircraft are not aware of this

And $(F1 \cap P2)$ is short for each of the following sub-conditions to apply:

- F1: Emergency from another a/c is received by ownship
- P2: Ownship pilot(s) are not aware of this.

Table 5a. Intent related (non-nominal) conditions for the hazards identified in Tallinn

T1.	P4 ∩ Q4, P5 ∩ Q5, P5, R5 ∩ Q5, R5
T2.	P1, R1
T3.	(A1 ∩ Q2), (B1 ∩ P2 ∩ Q2)
T4.	Is an A3 ConOps assumption
T5.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T6.	(A2 ∩ B2' ∩ P5 ∩ Q5)
T7.	(B4 ∩ P2 ∩ Q2)
T8.	n.a. (Not safety related)
T9.	(B4 ∩ P2 ∩ Q2)
T10.	(E1 ∩ R2), (F1 ∩ P2)
T11.	(B4 ∩ P2 ∩ Q2) (A^3 ConOps intentionally not yet designed for UAV's)
T12.	(B4 ∩ P2 ∩ Q2)
T13.	(A2 ∩ B2' ∩ P5 ∩ Q5)
T14.	(A1 ∩ P3 ∩ Q2), (B1 ∩ P2 ∩ Q2 ∩ R3)
T15.	(B4 ∩ P2 ∩ Q2), (A2 ∩ Q2), (B2 ∩ P2 ∩ Q2)
T16.	(A1 ∩ P1 ∩ Q2), (B1 ∩ P2 ∩ Q2 ∩ R1)
T17.	(B4' ∩ P4 ∩ Q4)
T18.	P1, P4, R1, R4
T19.	(B4' ∩ P4 ∩ Q4)
T20.	(A1 ∩ P1 ∩ Q2), (A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ R1 ∩ Q2), (B1 ∩ P2 ∩ R1 ∩ Q2)
T21.	n.a.
T22.	(A1 ∩ Q2), (B1 ∩ P2 ∩ Q2)
T23.	(A1 ∩ Q2), (B1 ∩ P2 ∩ Q2)
T24.	(A1 ∩ P1 ∩ Q2), (A4 ∩ Q2), (A2 ∩ P1 ∩ Q2), (B4 ∩ P2 ∩ Q2), (B1 ∩ P2 ∩ R1 ∩ Q2), (B2 ∩ P2 ∩ R1 ∩ Q2)
T25.	(A2 ∩ P1 ∩ P2), (B2 ∩ P2 ∩ R1 ∩ Q2)
T26.	(A2 ∩ P1 ∩ P2), (B2 ∩ P2 ∩ R1 ∩ Q2), (A2 ∩ B2' ∩ P5 ∩ Q5)
T27.	(A2 ∩ P1 ∩ P2), (B2 ∩ P2 ∩ R1 ∩ Q2), (A2 ∩ B2' ∩ P5 ∩ Q5)
T28.	A3, A4, B3, B4
T29.	A3, A4, B3, B4
T30.	A4, B4
T31.	(A1 ∩ P1 ∩ Q2), (A2 ∩ P1 ∩ Q2), (A4 ∩ P1 ∩ Q2), (B1 ∩ P2 ∩ Q2 ∩ R1), (B2 ∩ P2 ∩ Q2 ∩ R1), (B4 ∩ P2 ∩ Q2 ∩ R1),
T32.	(A2 ∩ B2' ∩ P5 ∩ Q5)
T33.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T34.	(A2 ∩ B2' ∩ P5 ∩ Q5)
T35.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T36.	(E1 ∩ A2 ∩ P1 ∩ Q2), (F1 ∩ B2 ∩ P2 ∩ Q2 ∩ R1), (E3 ∩ A2 ∩ P1 ∩ Q2), (F3 ∩ B2 ∩ P2 ∩ Q2 ∩ R1)
T37.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T38.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T39.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T40.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T41.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T42.	(A2 ∩ P1 ∩ Q2), (B2 ∩ P2 ∩ Q2 ∩ R1)
T43.	n.a.
T44.	n.a.
T45.	P4, R4

T46.	(A2∩B2'∩P5∩Q5)
T47.	Culture/Training/Experience/Individual
T48.	Culture/Training/Experience/Individual
T49.	Culture/Training/Experience/Individual
T50.	(A2∩B2'∩P5∩Q5)
T51.	n.a. (is a potential mitigating measure)
T52.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
T53.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
T54.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
T55.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
T56.	Out of scope (failure reporting issue)
T57.	P1, R1
T58.	P1, P2, P3, P4, P5, R1, R2, R3, R4, R5
T59.	Out of scope (failure reporting issue)

Table 5b. Intent related (non-nominal) conditions for the MFF2004 potential hazards

M1.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1), (A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M2.	(A1∩P1), (B1∩R1)
M3.	(A1∩P1), (B1∩R1)
M4.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1), (A1∩P1∩Q2), (B1∩P2∩Q2∩R1), P1, R1
M5.	n.a.
M6.	Out of scope
M7.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
M8.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1), (A1∩P1∩Q2), (B1∩P2∩Q2∩R1) (evaluated as boxiing-in example)
M9.	n.a.
M10.	n.a.
M11.	n.a. (ASAS-ACAS; Not intent related)
M12.	n.a. (ASAS-ACAS; Not intent related)
M13.	n.a. (ASAS-ACAS; Not intent related)
M14.	n.a. (ASAS-ACAS; Not intent related)
M15.	n.a. (ASAS-ACAS; Not intent related)
M16.	n.a. (ASAS-ACAS; Not intent related)
M17.	n.a. (ASAS-ACAS; Not intent related)
M18.	n.a. (ASAS-ACAS; Not intent related)
M19.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M20.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M21.	(E2∩ Q2), (F2∩P2∩Q2)
M22.	(E3∩P1∩ Q2), (F3∩P2∩Q2∩R1)
M23.	(E1∩P4), (F1∩R4)
M24.	(E2∩P1∩ Q2), (F2∩P2∩Q2∩R1)
M25.	(E3∩P1∩Q2), (F3∩P2∩Q2∩R1)
M26.	n.a.
M27.	n.a.
M28.	P2, R2
M29.	n.a. (Bit slower start-up)
M30.	P5, R5
M31.	P4, R4 (switching ASAS off; intentionally and unintentionally)
M32.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)

M33.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M34.	n.a.
M35.	P5, R5
M36.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M37.	P5, R5
M38.	E1, F1 (induces fuel problems)
M39.	n.a. (Not ASAS related)
M40.	n.a.
M41.	n.a
M42.	(E1∩F1)
M43.	Q2, (P2∩Q2)
M44.	Q2, (P2∩Q2)
M45.	(E3∩P1∩Q2), (F3∩P2∩Q2∩R1)
M46.	(E3∩P1∩Q2), (F3∩P2∩Q2∩R1)
M47.	(E2∩P1∩Q2), (F2∩P2∩Q2∩R1)
M48.	n.a. (Out of scope)
M49.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
M50.	(B4∩P2∩Q2), (B4'∩P4∩Q4), (B1∩P2∩Q2)
M51.	(A1∩Q2), (B1∩P2∩Q2)
M52.	(A1∩Q2), (B1∩P2∩Q2)
M53.	Delay by pilots
M54.	(E1∩A1∩Q2), (F1∩B1∩P2∩Q2)
M55.	(A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
M56.	P4, R4
M57.	(A1∩Q2), (B1∩P2∩Q2) (intentionally assumed)
M58.	n.a. (Out of scope)
M59.	n.a.
M60.	(E3∩P1∩Q2), (F3∩P2∩Q2∩R1)
M61.	(E3∩P1∩Q2), (F3∩P2∩Q2∩R1)
M62.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M63.	n.a. (Not ASAS specific)
M64.	Out of scope
M65.	(E1∩R2), (F1∩P2)
M66.	P4, R4
M67.	(E1∩F1)
M68.	P1, R1
M69.	Not intent related
M70.	P1, R1
M71.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1)
M72.	A4, B4
M73.	(A1∩P1∩Q2), (B1∩P2∩Q2∩R1), (A2∩P1∩Q2), (B2∩P2∩Q2∩R1)
M74.	(A4∩Q2), (B4∩P2∩Q2)
M75.	(A4∩B4'∩P4∩Q4)
M76.	P5, R5
M77.	n.a. (Out of scope of this safety analysis (military airspace is restricted airspace))
M78.	TCAS related
M79.	(A1∩P1∩Q2), (A2∩P1∩Q2), (B1∩P2∩Q2∩R1), (B2∩P2∩Q2∩R1)
M80.	n.a.

4.2 Clustering and ranking of intent related (non-nominal) conditions

The next step is to cluster individual hazards from Tables 1 and 3 on the basis of intent related (non-nominal) conditions in Tables 5a and 5b. Table 6a shows, in ranking order, how often each of these (combinations of) intent related (non-nominal) conditions apply. The individual hazard numbers are also shows per intent related (non-nominal) condition. Table 6b shows the same ranking of intent related (non-nominal) conditions, but now with a short description of this condition.

Four intent related (non-nominal) conditions (numbers 1-4) have been identified more then 15 times. These four conditions cover situations that the intent of ownship or of another aircraft is either not viable or not conflict free, whereas none of the crews are aware of this.

Subsequently there are twelve intent related (non-nominal) conditions (numbers 5-16) that are more complicated, and each of which has been identified between 5 and 10 times. Number 5 concerns the situation that one of the aircraft does not send its new intent, whereas the other aircraft are not aware of this. Number 6 concerns the situation that own intent and intents of multiple other aircraft are not viable. Numbers 7 and 8 concern fake emergency broadcastings that have intentionally been created by ownship crew or by one of the other crews. Numbers 9 and 10 concern (non-nominal) situations that the emergency of own or another aircraft is not broadcasted and/or not received. Next, there are six intent related (non-nominal) conditions (numbers 11–16) where the intent related (non-nominal) condition concerns the SA of one or more crews only. Hence these are (non-nominal) conditions under which everything is working well, but one or more crews have another or an incomplete intent SA. The problem is that under such a condition a crew may have problems to understand why airborne support systems are proposing to implement particular resolutions. And as long as the crew does not become aware of own SA mismatch, then it is difficult for the crew to accept a proposed resolution as long as it looks unacceptable to the crew.

Then there are 18 (non-nominal) conditions each of which has been identified between two and four times. These vary from one aircraft sending a fake emergency (#17 and #18), to an intent exchange which does not work well (#19), and to a condition that both ownship and another aircraft having an emergency (# 24).

Finally there is a sequence of 23 (non-nominal) conditions each of which has been identified only once. Because several of these may be quite risky if they happen, the mere fact that they have been identified only once in hazard brainstorms does not mean that their risk may be negligible.

Table 6a. Ranking of (combinations of) intent related (non-nominal) conditions

Rank Class	Hazard #
1. (B2∩P2∩Q2∩R1)	T5,T20,T24,T25,T26,T27, T31,T33,T36,T37,T38,T39,T40,T41,T42, T52,T53,T54,T55,M1,M4,M7,M8,M49,M55,M73,M79
2. (A2∩P1∩Q2)	T5,T20,T24,T25,T26,T27,T31,T33,T36,T37,T38,T39,T40,T41,T42, T52,T53,T54,T55,M1,M4,M7,M8,M49,M55,M73,M79
3. (A1∩P1∩Q2)	T16,T20,T24,T31,M1,M4,M8,M19,M20,M32,M33,M36,M62, M71,M73,M79
4. (B1∩P2∩Q2∩R1)	T16,T20,T24,T31,M1,M4,M8,M19,M20,M32,M33,M36,M62, M71,M73,M79
5. (B4∩P2∩Q2)	T7,T9,T11,T12,T15,T24,M50,M74
6. (A2∩B2'∩P5∩Q5)	T6,T13,T26,T27,T32,T34,T46,T50
7. (B1∩P2∩Q2)	T3,T22,T23,M50,M51,M52,M57
8. (A1∩Q2)	T3,T22,T23,M51,M52,M57
9. (F3∩P2∩Q2∩R1)	M22,M25,M45,M46,M60,M61
10. (E3∩P1∩Q2)	M22,M25,M45,M46,M60,M61
11. P1	T2,T18,T57,T58,M68,M70
12. R1	T2,T18,T57,T58,M68,M70
13. P4	T18,T45,M31,M56,M66
14. R4	T18,T45,T58,M31,M56,M66
15. P5	T1,T58,M30,M35,M37,M76
16. R5	T1,T58,M30,M35,M37,M76
17. A4	T28,T29,T30,M72
18. B4	T28,T29,T30,M72
19. (B4'∩P4∩Q4)	T17,T19,M50
20. (F2∩P2∩Q2∩R1)	M24,M47
21. (E2∩P1∩Q2)	M24,M47
22. (A4∩Q2)	T24,M74
23. (E1∩R2)	T10,M65
24. (E1∩F1)	M42,M67
25. (F1∩P2)	T10,M65
26. (P4∩Q4)	T1,T58
27. (A1∩P1)	M2,M3
28. (B1∩R1)	M2,M3
29. P2	T58,M28
30. R2	T58,M28
31. Q2	M43,M44
32. (P2∩Q2)	M43,M44
33. A3	T28,T29
34. B3	T28,T29
35. (F1∩B2∩P2∩Q2∩R1)	T36
36. (F3∩B2∩P2∩Q2∩R1)	T36
37. (E1∩A2∩P1∩Q2)	T36
38. (E3∩A2∩P1∩Q2)	T36
39. (F1∩B1∩P2∩Q2)	M54
40. (B1∩P2∩Q2∩R3)	T14
41. (B4∩P2∩Q2∩R1)	T31
42. (A4∩B4'∩P4∩Q4)	M75

43. (E1 ∩ A1 ∩ Q2)	M54
44. (A1 ∩ P3 ∩ Q2)	T14
45. (B2 ∩ P2 ∩ Q2)	T15
46. (A4 ∩ P1 ∩ Q2)	T31
47. (F2 ∩ P2 ∩ Q2)	M21
48. (E1 ∩ P4)	M23
49. (F1 ∩ R4)	M23
50. (P5 ∩ Q5)	T1
51. (A2 ∩ Q2)	T15
52. (E2 ∩ Q2)	M21
53. E1	M38
54. F1	M38
55. Q5	T1
56. P3	T58
57. R3	T58

Table 6b. Short description of ranked intent related (non-nominal) conditions

Rank	Class	Short description
1.	(B2 ∩ P2 ∩ Q2 ∩ R1)	Another a/c intent is not viable and nobody is aware
2.	(A2 ∩ P1 ∩ Q2)	Own a/c intent is not viable and nobody is aware
3.	(A1 ∩ P1 ∩ Q2)	Own a/c intent is not conflict free over MTCH and nobody is aware
4.	(B1 ∩ P2 ∩ Q2 ∩ R1)	Another a/c intent is not conflict free; nobody is aware
5.	(B4 ∩ P2 ∩ Q2)	Another a/c does not send intent and nobody is aware
6.	(A2 ∩ B2' ∩ P5 ∩ Q5)	Own and multiple a/c have non-viable intents and nobody is aware
7.	(B1 ∩ P2 ∩ Q2)	Another a/c intent intentionally not conflict free; others are not aware
8.	(A1 ∩ Q2)	Own a/c intent intentionally is not conflict free; others are not aware
9.	(F3 ∩ P2 ∩ Q2 ∩ R1)	Emergency of another a/c not received
10.	(E3 ∩ P1 ∩ Q2)	Emergency of own aircraft not broadcasted/not received by other a/c
11.	P1	Own crew lost SA of own a/c
12.	R1	Another crew lost SA of their a/c
13.	P4	Own crew lost SA of multiple other a/c
14.	R4	Another crew lost SA of multiple a/c
15.	P5	Own pilot SA differs from own and multiple other a/c
16.	R5	Another crew lost SA of own and multiple other a/c
17.	A4	Intent of ownship aircraft not broadcasted
18.	B4	Intent of one other aircraft not received
19.	(B4' ∩ P4 ∩ Q4)	New intents of multiple a/c not received and crew does not know
20.	(F2 ∩ P2 ∩ Q2 ∩ R1)	Another a/c sends fake emergency
21.	(E2 ∩ P1 ∩ Q2)	Own aircraft sends fake emergency
22.	(A4 ∩ Q2)	Own a/c intent is not broadcasted; thus not known to other a/c
23.	(E1 ∩ R2)	Ownship emergency switched on during conflict
24.	(E1 ∩ F1)	Both own and another a/c have emergency
25.	(F1 ∩ P2)	Another a/c emergency switched on during conflict
26.	(P4 ∩ Q4)	Own and multiple other a/c lost SA of multiple other a/c intents
27.	(A1 ∩ P1)	Own intent is not conflict free but own crew believes otherwise
28.	(B1 ∩ R1)	Another aircraft intent is not conflict free but crew believes otherwise
29.	P2	Own crew has SA difference for another a/c

30.	R2	Ownship state/intent is not properly perceived by encountering crew.
31.	Q2	Multiple other crews have an SA which differs for their aircraft
32.	(P2 ∩ Q2)	Ownship and multiple other crews have an SA which differs for one other aircraft
33.	A3	Own a/c autopilot set-point is broadcasted
34.	B3	Autopilot set-point of one other aircraft received
35.	(F1 ∩ B2 ∩ P2 ∩ Q2 ∩ R1)	Another a/c (partial) loss of control but emergency not received
36.	(F3 ∩ B2 ∩ P2 ∩ Q2 ∩ R1)	Another a/c (partial) loss of control and emergency received
37.	(E1 ∩ A2 ∩ P1 ∩ Q2)	(Partial) Loss of control and ownship emergency broadcasted
38.	(E3 ∩ A2 ∩ P1 ∩ Q2)	(Partial) Loss of control and ownship emergency not broadcasted
39.	(F1 ∩ B1 ∩ P2 ∩ Q2)	Another a/c sends fake emergency and its intent is not conflict free
40.	(B1 ∩ P2 ∩ Q2 ∩ R3)	One other crew wrongly applies rules of the air
41.	(B4 ∩ P2 ∩ Q2 ∩ R1)	One other aircraft intent not received and nobody aware
42.	(A4 ∩ B4' ∩ P4 ∩ Q4)	Intent exchange does not work well and nobody is aware
43.	(E1 ∩ A1 ∩ Q2)	Own a/c sends fake emergency and its intent is not conflict free
44.	(A1 ∩ P3 ∩ Q2)	Ownship crew wrongly applies rules of the air
45.	(B2 ∩ P2 ∩ Q2)	One other aircraft intent not viable and other aircraft crew are not aware
46.	(A4 ∩ P1 ∩ Q2)	Ownship intent not broadcasted/received and nobody aware
47.	(F2 ∩ P2 ∩ Q2)	Fake emergency broadcasted by one other aircraft and receiving aircraft are not aware
48.	(E1 ∩ P4)	Own a/c in emergency and own crew ignores all traffic
49.	(F1 ∩ R4)	Another a/c in emergency and its crew does not look at traffic.
50.	(P5 ∩ Q5)	Ownship and multiple other crews have an SA which differs for own and multiple other aircraft
51.	(A2 ∩ Q2)	Ownship intent not viable and other aircraft crew are not aware
52.	(E2 ∩ Q2)	Ownship fake emergency broadcasted and receiving aircraft are not aware
53.	E1	Own a/c emergency
54.	F1	Another a/c emergency
55.	Q5	Multiple crews have an SA which differs for own and multiple other aircraft
56.	P3	Ownship crew has an SA which differs for own and one other aircraft
57.	R3	Another crew has an SA which differs for their and one other aircraft

4.3 Initial assessment of consequences and frequency

For each of the intent related non-nominal conditions in Table 6, we develop an initial assessment of the consequences from the perspective of the A^3 ConOps. In doing so, we consider the following three types of intent related non-nominal conditions:

I. According to the A^3 ConOps design the non-nominal condition is typically handled within the Medium Term timeframe, by means of timely adaptation and broadcasting of properly adjusted intent. This applies to non-nominal conditions 1, 2, 6, 33, 34, 41, 45, 46, 51 53 and 54 and this covers 37 potential hazards. Of course there are exceptions in which it is not possible to adjust the intent within the Medium Term timeframe. In those cases the Flight Plan Conformance Monitoring (FPCM) of other aircraft will identify a mismatch between received intent and the trajectory flown. According to the A^3 ConOps in [D1.3], the applicable intent of the aircraft concerned will then be discarded by the onboard ASAS system. As a result the conflict resolution will be handled by the STCR system. The need for STCR resolutions for conditions #1, 2, 6, 33, 34, 41, 45, 46, 51, 53 and 54 are considered to form an exception on the rule. Based on a rough estimate this may happen in 10% of the cases where one of these non-nominal conditions apply.

II. These are those conditions for which the first line of defence, i.e. Medium Term Conflict Resolution can no longer solve the problem. According to the A^3 ConOps desing the handling of the non-nominal condition is now up to the Short Term Conflict Resolution line of defence. This concerns non-nominal conditions 3, 4, 5, 7, 8, 17, 18, 19, 22, 27, 28, 35, 36, 37, 38, 40, 42, 44, 49 and covers 41 potential hazards.

III. These are non-nominal conditions in which everything seems to be working well, but one or more crews have different or incomplete intent SA. The problem is that under such a condition a crew may not understand why airborne support systems are proposing to implement particular resolutions which are not consistent with their own SA. In those cases the crew may cast doubt about the proper working of the support systems rather than having the possibility to identify a shortcoming in their own SA. And as long as the crew remains suspicious about the proposed resolutions, valuable time may pass while no action is taken to solve the problem. This concerns non-nominal conditions 9-16, 20, 21, 23-26, 29, 30, 31, 32, 39, 43, 47, 48, 50, 52, 55, 56, 57 and covers 32 potential hazards.

For each of these three types of consequences a rough initial estimation of the frequency of their occurrence was performed. This initially estimated value is aimed to represent an order of magnitude only. Per type of consequences the frequency of occurrence has first been estimated for each non-nominal condition, and subsequently these estimated values have been accumulated to get an estimated frequency per type of consequences.

Type I: There are six (non-nominal) conditions. Based on two independent educated guesses (including a subsequent discussion and resolution of the differences), each condition is estimated to happen less than:

1. Once per 100 flights
2. Once per 100 flights
6. Once per 100 flights
33. Once per 1000 flights
34. Once per 1000 flights
41. Once per 1000 flights
45. Once per 1000 flights
46. Once per 1000 flights
51. Once per 1000 flights
53. Once per 1000 flights
54. Once per 1000 flights

Intent related non-nominal conditions 1, 2 and 6 are roughly estimated to happen once per 100 flights or less. Six other conditions are roughly estimated to happen once per 1000 flights or less, and two conditions are estimated to happen once per 10,000 flights or less. In total this comes down to an estimated maximum frequency of 3.62 or less type I intent related non-nominal conditions per 100 flights. If we assume that one out of ten fails to be resolved by the first line of defence (MTCR) then the estimated maximum frequency of 0.36 type I intent related non-nominal conditions lead to a conflict that has to be resolved by STCR.

Type II: Based on educated guesses, this is expected to happen less than
3. Once per 100 flights
4. Once per 100 flights
5. Once per 1000 flights
7. Once per 100 flights
8. Once per 100 flights
17. Once per 100 flights
18. Once per 100 flights
19. Once per 100 flights
22. Once per 1000 flights
27. Once per 1000 flights
28. Once per 1000 flights
35. Once per 1000 flights
36. Once per 1000 flights
37. Once per 1000 flights
38. Once per 1000 flights
40. Once per 10000 flights
42. Once per 100 flights
44. Once per 10000 flights
49. Once per 1000 flights

For six intent related non-nominal conditions (3, 4, 7, 8, 17, 18, 19 and 42) each is roughly estimated to happen once per 100 flights or less. For nine other conditions, each is roughly estimated to happen once per 1000 flights or less. Two conditions happen once per 10000 flights or less. In total this comes down to an estimated maximum frequency of 8.2 type II intent related non-nominal conditions per 100 flights.

Type III: Based on educated guesses, this is expected to happen less than
9. Once per 10000 flights

10. Once per 10000 flights
11. Once per 100 flights
12. Once per 100 flights
13. Once per 100 flights
14. Once per 100 flights
15. Once per 100 flights
16. Once per 100 flights
20. Once per 1000 flights
21. Once per 1000 flights
23. Once per 10000 flights
24. Once per 10000 flights
25. Once per 10000 flights
26 Once per 100 flights
29. Once per 100 flights
30. Once per 100 flights
31. Once per 10000 flights
32. Once per 10000 flights
39. Once per 1000 flights
43. Once per 1000 flights
47. Once per 10000 flights
48. Once per 10000 flights
50. Once per 100 flights
52. Once per 10000 flights
55. Once per 100 flights
56. Once per 1000 flights
57. Once per 1000 flights

For eleven intent related non-nominal conditions (11-16, 26, 29, 30, 50, 55) each is roughly estimated to happen once per 100 flights or less. For six conditions (20, 21, 39, 43, 56, 57) each is estimated to happen less than once in 1000 flights. For the ten other conditions, each is roughly estimated to happen once per 10,000 flights or less. In total this comes down to an estimated maximum frequency of 11.7 type III intent related non-nominal conditions per 100 flights.

In order to get a better view on Type III conditions, the question was asked ‘what the crew is expected to do for type III non-nominal conditions?’ Based on the A^3 ConOps this is expected to work as follows:

9: Conflict resolution depends on the second line of defence, which is STCR.
10: As long as crew does not become aware, STCR should resolve the conflict. When crew becomes aware; then emergency is announced through R/T.
11-14: Crew will regain SA by probing individual aircraft.
15-16: Crew will follow procedures, i.e. through accepting conflict free trajectory changes only.
20: Own aircraft is given priority. If crew becomes suspicious, then it makes note and reports.
21: Own aircraft gets priority from encountering aircraft. If encountering crew gets suspicious then they make note and report.
23: Other crew will solve conflict using STCR.
24: Conflict will be solved using MTCR, and subsequently by STCR in case MTCR is too late.

25: Most likely the crew will identify this in time, and then correct. If not, then STCR will form the second line of defence.
26: Crew will first regain SA of traffic by probing individual aircraft. As a consequence, the crew response to resolution proposed by support system takes more time, and the chance of error may increase.
29: Other aircraft crew should resolve conflict using STCR.
30: Own crew should solve conflict using STCR.
31: Effect is that other aircraft most likely will do more than normal in the medium and short term conflict resolution.
32: Effect is that other aircraft most likely will do more than normal in the medium and short term conflict resolution.
39: Crew will resolve conflict, and subsequently make note to report.
43: Other aircraft crew will resolve conflicts. Most likely they will also report.
47: Crew should give priority to emergency aircraft and resolve any conflict. Subsequently make note to report.
48: Crew will follow procedures, which means that another aircraft should solve the conflict using STCR.
50: Own and/or other aircraft should de-clutter the CDTI to regain required SA. De-clutter options should be made available
52: Emergency aircraft will get priority. Other aircraft will resolve any conflict, and make note to report.
55: Own and/or other aircraft should de-clutter the CDTI to regain required SA. De-clutter options should be made available
56: Crew should follow procedures
57: Crew should follow procedures

From the above, it appears that seven type III non-nominal conditions (9, 10, 23, 24, 29, 30, 47, 48 and 52) should be resolved by means of short term conflict resolution. With regard to the other 17 cases, it is estimated that in 10% of these cases MTCR will be too late to solve the conflict. This means that for type III non-nominal conditions 3.02 times per 100 flights conflict resolution will fall upon the STCR module.

If we accumulate the roughly estimated frequencies for Type I, Type II and Type III intent related non-nominal conditions that should be resolved by STCR, then this leads to the conclusion that less than once per ten flights (~ 0.36 + 8.2 + 3.02 = 11.58 per 100 flights), the MTCR will not be able to resolve the conflict and resolution will fall upon the STCR module.

4.4 Main intent related (non-nominal) conditions to improve A³ ConOps

As has been explained in the introduction, the current initial hazard analysis study has a dual purpose. The first purpose is to gain insight in the type of scenarios that should be considered in the sequel of the safety analysis, i.e. in WP7.3. The second purpose is that the initial hazard analysis results place the A^3 ConOps into a new perspective regarding safety. For any advanced concept design, it is important to become aware of the weakest links in the chain. This subsequently allows the designers to learn from this and subsequently improve their A^3 ConOps design for these weakest links.

On the basis of the initial hazard analysis outcomes, there are ten (non-nominal) intent related conditions (3, 4, 7, 8, 17, 18, 19, 29, 30, 42) that have been estimated to cause once per hundred flights that STCR line of defence should resolve the conflicts. These conditions are specified in Table 7. Potentially, these conditions form the weakest links in the A^3 ConOps design of WP1.

Table 7. Main intent related (non-nominal) conditions

Rank	Class	Description
3	(A1 ∩ P1 ∩ Q2)	Own a/c intent is not conflict free and nobody is aware
4	(B1 ∩ P2 ∩ Q2 ∩ R1)	Another a/c intent is not conflict free and nobody is aware
7	(B1 ∩ P2 ∩ Q2)	Another a/c intent intentionally not conflict free; others are not aware
8	(A1 ∩ Q2)	Own a/c intent intentionally is not conflict free; others are not aware
17	A4	Intent of ownship aircraft not broadcasted
18	B4	Intent of one other aircraft not received
19	(B4' ∩ P4 ∩ Q4)	New intents of multiple a/c not received and crew does not know
29	P2	Own crew has SA difference for another a/c
30	R2	Ownship state/intent is not properly perceived by encountering crew.
42	(A4 ∩ B4' ∩ P4 ∩ Q4)	Intent exchange does not work well and nobody is aware

Eight of the ten main intent related (non-nominal) conditions in Table 7 have to do with multi agent situation awareness differences. This means that each of this eight is of potential relevance to be addressed by WP4. In addition it is expected that WP9 tries to address the mitigation of all ten main conditions through the derivation of safety requirements. For WP8 the best that can be done is to start writing down in detail how the proposed A^3 ConOps is expected to work for each of these conditions, and to think of options that may exist for Flight Operations Centres (FOC's) in being of help to the mitigation of one or more of these main intent related conditions within the A^3 ConOps. And complementary to this, WP8.3 may consider what the options are for ATM on the ground when A^3 equipped aircraft are assumed to fly within the SESAR 2020 advanced concept.

Because the intent related (non-nominal) conditions in Table 7 have been assessed in a rather qualitative way, and the maximum frequency of occurrence and the worst consequences have been estimated using educated guesses, it may very well be the case that one or more of these conditions are much less risky or happen less frequently than we currently expect. The best way to find this out is to conduct Monte Carlo simulations of scenarios that include the main conditions of Table 7. Then it may become clear that not all of the conditions in Table 7 are as risky as our current pessimistic estimates are.

5 Concluding remarks

This report performed a hazard identification and initial hazard analysis for the A^3 operation which is described in iFly Deliverable D1.3 on the Autonomous Aircraft Advanced (A^3) ConOps [iFly D1.3]. The key outcome is the identification of ten (non-nominal) intent related conditions, which deserve dedicated attention by WP8 and WP9 with the aim of improving the A^3 ConOps for these conditions. Eight of the ten non-nominal conditions have to do with multi-agent SA differences, and such is roughly estimated to happen up to once per 10 flights or less. These eight deserve dedicated attention from WP4.

In parallel to this hazard identification and 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 should cover the human and technical agents, their interactions and both the nominal and non-nominal aspects of the operation. This will be reported in iFly deliverable D7.1c. Subsequently, Monte Carlo simulations will be performed to assess flight efficiency and collision risk of the A^3 operation. The scenarios considered will make use of the results obtained in this report. Eventually, the results will be reported in iFly Deliverables D7.3 and D7.4.

References

[Blom et al, 2009] 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.

[Daams, 1997] Daams, 1997, Free Flight Hazard Identification brainstorm session

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

[Everdij, 2001] Everdij, 2001, Minutes CARE-ASAS Activity 3 WP3.1 hazard brainstorm

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

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

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

[ICAO, 2003] ICAO (2003). Airborne separation assistance system (ASAS) circular, Draft, version 3, SCRSP, WGW/1 WP/5.0, International Civil Aviation Organization, May 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 , and Utartu (Aavo Luuk), Version 2.7 of 28 May 2009. 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 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 D7.2a] iFly Deliverable D7.2.a, Review of risk assessment status for air traffic, by H.A.P. Blom, J. Krystul, G.J. Bakker, M.B. Klompstra, B. Klein Obbink, S.H. Stroeve, H.H. de Jong, Draft version 1.0 of 14 January 2009. Available on iFly website http://ifly.nlr.nl/

[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.

[Klein Obbink, 2002] Klein Obbink, 2002, MFF Self Separation Assurance OHA

[Klompstra, 2008a] Minutes of meeting of the iFly Pre-Brainstorm meeting Brainstorm held at the University of Tartu, Tallinn Office on 29 May 2008.

[Klompstra, 2008b] Minutes of meeting of the iFly Brainstorm held at the University of Tartu, Tallinn Office on 30 May 2008.

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

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

[MFF, 2004] MFF, 2004, Hazards identified during the Amsterdam February 2004 MFF experiments

[MFF, 2005] MFF (2005), MFF Final safety case, Report MFF D734, ed. 1.0. Available at http://www.medff.it/public/index.asp, November 2005.

[NASA, 1999] NASA (1999). 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 (2004). 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.

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