HYBRIDGE

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

WP9: Risk assessment for a distributed control system

Description of advanced operation: Free Flight

Bart Klein Obbink

7th March 2005

Version: *1.0*
Task number: *9.1*
Deliverable number: *N/A.*
Contract: *IST-2001-32460 of European Commission*

DOCUMENT CONTROL SHEET

Title of document: *Description of advanced operation: Free Flight*

Authors of document: *B. Klein Obbink*

Deliverable number: *N/A.*

Contract: *IST-2001-32460 of European Commission*

Project: *Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design (HYBRIDGE)*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
0.1	23th Dec. 2003	All	1st draft: creation of document
0.2	23th Jan. 2004	All	First chapter added
0.3	16th Feb. 2004	All	A new first chapter added
0.4	31s Mar. 2004	All	NLR Review comment
0.5	5th May 2004	References	References improved
0.6	11th May 2004	All	UPAT review comment
0.7	26th Dec. 2004	4,5, References	EEC review comment
1.0	7th March 2005	2,3,4,5,8, Appendix	NLR review comment

Version 0.1		Organisation	Signature/Date
Authors	Bart Klein Obbink	NLR	
Internal reviewers	Henk Blom,	NLR	
	Margriet Klompstra	NLR	
	John Lygeros	UPAT	
	Eric Hoffman	EEC	

Abstract

In WP 9 of the Hybridge project, a risk assessment for a distributed ATM operation is executed, based on a stochastic hybrid model for the operation. In this first report of the WP, the selected ATM operation, called Free Flight, is introduced. Not only the operation itself is described, also its environment, the required functionalities and the traffic information flow. The report starts with a chapter explaining why Free Flight is considered the appropriate choice for the consecutive steps to be executed in WP 9, taking into account the objectives of the project and the WP itself.

CONTENTS

1. Introduction

Background of Hybridge project

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

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

Background of WP 9

The objective of Workpackage 9 is to demonstrate how the various developments in other Hybridge work packages contribute to a safe advanced air traffic operation which makes explicit use of distributed control over multiple aircraft. In doing so, developments from other work packages are combined either in the definition of the air traffic operation to be assessed, or in the execution of the risk assessment.

The work is organised in the following sequence of tasks:
Task 9.1: Identify the advanced air traffic operation, including a systematic identification of all non-nominal situations and hazards. For the advanced air traffic operation we will consider one in which it is expected that the proper co-ordination between air and ground in conflict resolution is an essential condition for realising significant capacity improvements. Potential applications are closely spaced runway situations at a busy airport and collaborative airborne separation assurance in dense en-route or TMA traffic areas.
Task 9.2: Develop a mathematically unambiguous stochastic hybrid model for the operation considered, and specify all model assumptions made, all model parameters and their values that are introduced. In view of the complexity of the development of such a mathematical model an existing model instantiation in Dynamically Coloured Petri Net (DCPN) form will be used as starting point, and all improvements will be developed in an iterative way: extend model specification, update assumptions and update list of model parameters and their values.
Task 9.3: Develop appropriate risk decomposition and uncertainty assessment approaches. For this, use is made of the methods developed in WP8. Subsequently extend already available accident risk evaluation software according to the model instantiation and risk decomposition of Tasks 9.2 and 9.3.
Task 9.4: Perform the risk assessment with support of stochastic analysis and Monte Carlo simulations for the instantiated models and their software implementation, and assess how sensitive the risk result is for changes in the values of the most relevant parameters.
In each of these tasks the scalability with increasing complexity is addressed.
Task 9.5: Produce and present Scientific paper(s)

Relations to other workpackages

The aim of Workpackages 2 and 8 is to develop novel methods for the modelling and decomposition of risk such that extreme low risk values can be modelled through hybrid stochastic models and assessed through Monte Carlo simulations. These methods are directly applicable in Workpackage 9. The aim of Workpackage 10 is to develop courses on stochastic analysis based ATM risk assessment. The results of and lessons learned in Workpackage 9 might serve as illustrative material.

The other Workpackages have a more loose relation to WP 9. It might be possible to replace the standard Free Flight algorithms by the conflict detection and resolution algorithms that are developed in Workpackage 6 [D6.2] study the effect of this replacement on safety, although the later algorithms are not yet sufficiently mature. The objective of Workpackage 5, to extend the hierarchical and model predictive control techniques to stochastic hybrid systems, is also not mature yet [D5.1]. The results of Workpackages 5 and 6 will be discussed within WP 9.4, when considering other operational concepts and model structural assumptions. The Workpackage 1 and 3 results go through Workpackages 5 and 6. . The Workpackage 4 and 7 results are not sufficiently mature yet [D4.2], [D7.3].

Table 1 Relation of WP9 to other Workpackages

Workpackage	Where to be used by Workpackage 9
WP 1	Via WP5
WP 2	Direct to WP 9.2
WP 3	Via WP5
WP 4	Not applicable
WP 5	Direct to WP 9.4
WP 6	Direct to WP 9.4
WP 7	Not applicable
WP 8	Direct to WP 9.3

Background of Task 9.1 and this report

The main goal of Task 9.1 is to identify an advanced ATM operation that is suited for further analysis, as described in the sections above.

In Section 2, the appropriate advanced ATM operation, called Free Flight, is identified and described in Section 3. The scope of the Free Flight operation considered is given in Section 4. Sections 5, 6 and 7 describe the details of the operation. Section 8 describes the hazard identification performed.

2. Identification of advanced operation

Criteria for selection

The objective of WP 9 is to demonstrate how the various developments in other workpackages contribute to safety management, by performing a safety assessment of an advanced ATM operation. Free Flight is selected as the most appropriate advanced ATM to investigate, considering Hybridge's objectives. This is explained by the sections below, first introducing the concept quickly, and then highlighting its characteristics and the challenges of the required accident risk assessment.

Advanced ATM: Free Flight

Current Air Traffic Management systems are based on the assumption that aircraft cannot detect each other accurately enough to avoid collisions with other aircraft. As a result, control and management of most airspaces in the civil air transport system is centralised: Air Traffic Control has the responsibility to separate aircraft from each other.

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

Characteristics of the operation

In the paragraphs below, some characteristics of the operation are highlighted from the point of view of the Hybridge objectives and the relationship to other workpackages.

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

The Free Flight concept is not completely fixed yet with respect to all details of procedures, algorithms, equipment performance requirements, etcetera. Actually, ATM concept designers are still debating implementation choices; and collision risk is an important qualifier in that discussion because of the air transport's safety criticality. One implementation choice is the level of co-ordination between aircraft (such as the need for confirmation of the conflict or for exchange of intended trajectories). Another aspect is whether the conflict resolution concept should be based on priority rules or on co-operative contributions. Such choices can be considered as control mechanisms in a distributed architecture.

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

Accident risk assessment

Although preliminary results show that Free Flight may be safe, it is not clear under which maximum traffic flows safety applies. And there is some scepticism in the ATM community about the safety of the concept at traffic levels encountered over Europe. The absolute need for evidence of safety in new concepts in air transport systems then explains the need for an integrated safety assessment of the Free Flight concept, recognising that improving ATM safety is more than making sure that all individual ATM elements function safely. In the paragraphs below, some characteristics of the accident risk assessment are highlighted from the point of view of the Hybridge objectives and the relationship to other workpackages.

The operation can be modelled as a hybrid system, with continuous dynamics in e.g. the physical trajectories of the involved aircraft and discrete dynamics in e.g. the state of system components. The nature of the operation (systems that may unexpectedly go down, navigation errors increasing in time, humans operators making errors, etcetera) require a stochastic approach.

Apart from the dynamics of each component of the system, the interactions between components are the key for a proper modelling of the system. Special attention should be paid to the traffic information exchange, as lack or inconsistency of the traffic information might lead to catastrophes. In that respect, the pilot’s situational awareness and the human cognition performance error evolution should be taken into account.

Some of the intrinsic characteristics of the operation mentioned in the section above make the accident risk assessment particularly challenging. Again, there is the highly distributed nature of the system. Besides, in an adequate approach, the safety effects of levels of co-ordination and automation are traceable in the results of the risk assessment ([Hybridge]).

This all requires a distributed control theory for safety critical operation, embedded within safety management and a risk assessment methodology based on stochastic analysis.

3. General introduction to Free Flight

Background and benefits of Free Flight

In the very early days of flying, all pilots navigated using ground features such as roads, rail tracks and coastlines. By keeping a sharp look out, collisions were avoided by the pilot using some rules indicating who had right of way. Later on, radar and radio allowed control towers to separate traffic in weather conditions previously inhibiting flight. Air Traffic Control became responsible for the separation of aircraft during the complete flight except for some general aviation. In the meantime, beacons placed all over the country created a route structure in the sky consisting of so-called airways. This route structure is still being used today although modern navigation no longer relies on flying to and from a beacon. Current Air Traffic Control is thus developed from old technologies, based on:

- A set of rules in the sky: the IFR,
- Air Traffic Controllers who, for their section, are responsible for separation,
- Ground surveillance by means of (secondary) radar and information processing systems,
- Communication by R/T,
- A system for alerting the ATCo for conflict on the short term: STCA,
- A system for alerting the aircrew for conflict on the short term: TCAS.

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

The concept might bring the following direct benefits:

- Aircraft can fly their optimal trajectory (i.e. choose route, flight level and speed), thus minimising flight time or fuel consumption,
- The risk on mid-air collisions might be reduced, as the local traffic density is decreased and as the actions to prevent conflicts are distributed among more actors while requiring less information layers,
- The En Route capacity can be increased, thus reducing delays and eliminating airspace capacity limitations.

Free Flight is enabled by several techniques. The main ingredients are a reliable and accurate airborne navigation system like GNS, airborne surveillance based on e.g. ADS-B and ASAS, the general name for an aircraft system that provides support to the flight crew in order to separate their aircraft from other aircraft. The functionality of ASAS at least includes modules for Conflict Detection and Conflict Resolution. All information that is appropriate to present visually is shown on what is called a Cockpit Display of Traffic Information, a CDTI.

To assure effective assurance, several proposals have been made about priority principles, rules for conflict solving sequence determination and explicit co-ordination procedures to confirm conflicts and to anticipate manoeuvres. However, it looks like most of this turned out not to be necessary. Actually, there is a tendency to make the concept quite lean and mean, in order to avoid much information exchange, while keeping it comprehensible and safe.

Free Flight Safety Assessment

Despite the empirical fact that Free Flight is working fine in test beds, everybody agrees that a lot of things need to be done before it can be implemented operationally. Most scepticism can be placed under one of the following bullets, which will be discussed below shortly:

- Free Flight is technically impossible,
- Free Flight is politically unacceptable,
- Free Flight is unsafe.

This report assists the activities that elaborate on the safety of Free Flight. Although preliminary results show that Free Flight is as potentially safe as current ATM, its safety is certainly not proved. Serious analysis needs to be done ([SAF-ASAS], [Brooker]), as the concept is so different from the current air transport system, which safety is above believe. A full risk assessment will not only include a functional hazard identification with consecutively deducing safety and interoperability requirements, but most go deeper and should model the distributed interactions at different time scales between humans, equipment, procedures and the environment. As the pilot's situational awareness plays such an essential role in the concept, information flow processes and human cognition performance error evolution should be taken into account.

4. Scope of Free Flight operation considered

Safety aspects

In the context of this WP 9 study, the safety aspect considered is mid-air collisions. The probability of mid-air collisions will be expressed quantitatively per flight hour per aircraft, building on results in WP 2 and WP 8 [D2.2], [D8.3], [D8.4].

When it comes to safety, both ICAO and the Safety Regulation Commision within Eurocontrol specify TLS values agianst which procedures have to be judged safe without considering the effect of the ACAS safety net [SRC 2], [PO-ASAS], [SAF-ASAS]. This way of looking to ACAS autonomous role does not imply necessarily that ACAS should be independent from ASAS equipment or procedures. However, this kind of independence is sometimes implicitly referred to, in statements as in [Abeloos]: “A requirement from the ASAS point of view is that there must be an independent backup system for ASAS failure. That is exactly what the TCAS is designed for: to prevent collision when the primary means of separation assurance has failed”.

Transitions into or out of FFAS are not taken into the risk assessment, as if the FFAS is infinite and as if surrounding Managed Airspaces (MAS), transition zones, SUA’s and TSA do not exist. The FFAS has therefore no substructure and is homogeneous. Notwithstanding this, a particular emergency procedure states that under circumstances an aircraft should leave the FFAS. This is simply modelled by assuming the aircraft is descending to FL 280 or below, and that no collision take place after passing this FL.

Open issues

If the Free Flight concept would have been completely fixed, the result of our study would be one assessment of the expected accident risk, averaged over all kind of encounters. However, as the concept and realisation are still in the phase of improvement, the concept designers would like to base parts of their design on what is actually the safest choice. Therefore the set-up of the model used for the collision risk assessment should be sufficient open and flexible to incorporate the following issues.

Issue 1. Broadcasting intent information; that is: sending out the first 4-D Trajectory Change Point, such that other aircraft can process this piece of information in the Conflict Prevention and Conflict Detection. The default assumption is that intent information is not broadcast.

Issue 2. The RNP-value, the separation minima and the look-ahead time. The default assumption is that the RNP-value is 1. A first choice on the basis of previous studies [CARE/ASAS WP3] is a vertical separation of 1000 ft and a horizontal separation of 5 Nm. The default assumption is that ASAS detects a conflict if the separation minima will be violated within 5 minutes.

Issue 3. A split of the conflict resolution process in a priority and a co-operative phase. The default assumption is that the conflict resolution phase is split into two phases: in a first phase one aircraft gets priority while the crew of the other aircraft should make a resolution manoeuvre and in a second phases both crews should make a resolution manoeuvre.

Issue 4. Co-ordination of conflict resolution; that is once an aircraft detects a conflict, it is communicated whether a resolution manoeuvre will be executed (which depends among other things whether the other involved aircraft detected a conflict too) and if so, which resolution manoeuvre will be executed. The default assumption is that co-ordination does not take place explicitly.

5. Description of airspace, traffic and equipment

Free Flight Airspace Characteristics

Free Flight Airspace (FFAS) is an en-route airspace without fixed routes or an active ATC specifying routes: the pilots have the freedom to select their path, flight level and speed in real time, only limited by their responsibility to maintain airborne separation.

FFAS is assumed to start at FL 280 and is not limited from above. The airspace below is a Managed Airspace (MAS), where aircraft in emergency can descend into.

FFAS is assumed to stretch out infinitely in the horizontal directions; there are no surrounding Managed Airspace (MAS), transition zones, SUA's and TSA. The actual FFAS has no substructure and is homogeneous.

Only fully ASAS-equipped aircraft with qualified crew have access to the FFAS.

Free Flight Separation Minima

The airborne separation minima are expressed as a vertical separation in ft and a horizontal separation in Nm, giving the aircraft's protected zone a cylindrical geometry. The two values are considered as variable quantities in the safety assessment. The default choice on the basis of previous studies [CARE/ASAS WP3] is a vertical separation of 1000 ft and a horizontal separation of 5 Nm.

In order to study the effect of the separation minima in Study 2, it is in some cases assumed that aircraft have a minimal horizontal separation of 2.5 or 10 Nm, and a minimal vertical separation of 500 feet or 2000 ft.

ATC role in Free Flight

Air Traffic Control (ATC) has the authority to give or refuse aircraft access into the FFAS. In principle, ATC refuses aircraft if and only if one of the following criteria applies:

- The local traffic density is too high.
- The aircraft or their crew do not comply with the Airworthiness Criteria.
- The air operator is not certified, implying that the aeroplane does not have a standard Certificate of Airworthiness that the relevant equipment (as ADS-B, GNS and ASAS) is certificated and that the crew is qualified to execute Free Flight.

AOC role in Free Flight

The aircrew can try to optimise their trajectory, due to the enlarged freedom to choose path and flight level. Airline Operational Centre (AOC) of the crew's airline company might indicate a preference as a timed arrival, minimised flight time, or fuel consumption. Moreover, the Airline Operational Centre might assist the crew by providing information on the traffic and weather circumstances or by determining the actual best trajectory.

Weather characteristics

The weather characteristics correspond to the climate of the Northern Atlantic Region.

Traffic Characteristics

Because of the lack of any route structure within the FFAS, the traffic within it cannot be compared with the ATC controlled traffic flows of today. It is stated ([Hoekstra]) that the main effects of going from fixed route structured airspace to free route structured airspace can be:

- The frequency of aircraft encounters per aircraft is reduced significantly,
- The complexity of the traffic flow is increased significantly.

The actual traffic spread is assumed to correspond to the current air traffic spread above Western Europe. The aircraft mix corresponds to the current aircraft mix at altitudes above in the Western European airspace above FL 280.

The capacity of a FFAS has to be determined by the capability of aircrew for self-separation, and this is related to the extent to which Free Flight is safe. Once the capacity is known, it can be translated in a maximally allowable local traffic density, expressed in number of aircraft per volume or area. It is then the ATC's task to monitor the amount of traffic in a specific local area and to refuse access to a saturated FFAS. Although uncertain yet, it is assumed that the maximally allowable local traffic density is three times the current averaged air traffic density above Western Europe.

Aircraft CNS Equipment

Only fully ASAS-equipped aircraft with qualified crew have access to the FFAS. ATC has the authority to give or refuse aircraft access into the FFAS .

Aircraft onboard system requirements are mainly based on [OCD], [MOPS ASSAS], [MOPS CDTI] and [RTCA CO CM].

Navigation

Navigation is Global Navigation Satellite System (GNSS)-based, augmented and coupled with INS/IRS. Aircraft are assumed to be capable for RNP1. In case of failures, INS/IRS and, depending on the ground infrastructure, traditional systems as VOR, DME and NDB are available.

Altitude is determined by means of several independent altimeters.

In order to study the effect of the RNP value in Study 2, it is in some cases assumed that aircraft have RNP-½, RNP-2 or RNP-5 navigation capability.

Communication

The concept of Free Flight requires automatic inter-aircraft communication of, at least, aircraft's identity, position and velocity. Aircraft are supposed to be equipped with ADS-B, a system that periodically broadcasts and continuously receives this information from other aircraft. The [ICAO Data Link application] gives the following definition: ADS-B is a surveillance application transmitting parameters, such as position, track and ground speed, via a broadcast mode data link and at specified intervals, for utilisation by any air and/or ground users requiring it. The aircraft originating the broadcast has no knowledge of which systems are receiving the broadcast. Any air or ground based user may choose to receive and process this information. This definition does not mention explicitly the possibility to broadcast intent information via ADS-B, such as Trajectory Change Points.

It is required that at least the following information elements can be handled and provided by ADS-B:

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

Other information elements might also be sent out non-mandatory, such as Turn indication, Navigation uncertainty category or Estimated Time of Arrival (ETA) to exit point FFAS.

In order to study the effect of intent information in Study 1, it is assumed that aircraft send the first 4-D Trajectory Change Point, such that other aircraft can process this piece of information in the Conflict Prevention and Conflict Detection. The default assumption is that this intent information is not broadcast.

Concerning the equipment that transfers data over air to air paths, there are several technologies available, such as Extended squitter, VDL Mode 4, UAT, and JTIDS/MIDS, each with its own benefits and limitations.

In addition, the aircraft are equipped with standard R/T to ensure voice communications for (at least) non-routine and emergency use, for aircraft-aircraft and for aircraft-ATC communication.

Surveillance

Airborne surveillance data will be processed to form tracks of other aircraft to be presented on the cockpit display (CDTI). It is anticipated that airborne surveillance will exclusively rely on ADS-B. This implies that in case of a full or partial ADS-B failure, ground-to-air data-link like TIS-B could in general not be used as a complementary source.

The datacommunication bearer technique for ADS-B is unspecified. It is assumed that there are dedicated and separate ADS-B transmitters and receivers.

ACAS also provides surveillance means and is described in the last subsection below.

ASAS and CDTI

ASAS itself might be considered to be a system processing the information flows from the communication links, the navigation systems, the FMS and the auto-pilot. It contains several hardware and software components, depending on the application to be served apart from Free Flight. There is the traffic information processing function, that processes the raw data to generate information streams into for example a display. ASAS encompasses other functionalities (as conflict detection and resolution) that are not described in this paragraph. A control panel is the interface between the pilot, the display and the data processing, enabling the pilot to select the preferred features.

The CDTI is the general name for the display supporting the ASAS and ADS-B derived applications. It can contain traffic information, selected waypoints, weather information, an airport map, proposed manoeuvres, virtual tunnels in the sky to guide the pilot, etceteras. The task of the CDTI is to inform the crew of the traffic around the aircraft, and aid them in the conflict handling. In particular, the CDTI shall enable the crew to monitor traffic by:

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

The CDTI should therefore:

- Show conflict zones.
- Show dangerous areas.
- Show specific areas in FFAS: segregated areas, transition zones, density of traffic in entry/exit points.
- Show FFAS boundaries.
- Show forbidden headings, climb/descent sense and rates, speed ranges so as to avoid short-term conflicts.

So, ASAS collects airborne surveillance data via ADS-B, thus based on the other aircraft's navigation. The data will be processed (e.g. filtered) to form tracks of other aircraft to be presented on CDTI and, in combination with own aircraft's navigation and intent data, used to develop information on targets relative to own aircraft. In this way potential conflict situations can be identified. ASAS also provides a means for post flight analysis of traffic situations and conflicts.

The CDTI is assumed to be consistent with the rest of the flight deck in terms of color, standardization, automation, symbology, interaction techniques and operating philosophy. The CDTI may often be used in coordination with other systems, such as for example other Caution and Warning Systems, ACAS, Autoflight systems and FMS [ARP 5365].

ACAS

ACAS is the ICAO generic term for an airborne collision avoidance system that uses interrogations of, and replies from, other aircraft's transponders, and which operates independently of ground based equipment. The official definition reads: an aircraft system based on secondary surveillance radar transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with secondary surveillance radar transponders.

In [Hawkes], an acceptable installation for ACAS is described. The most important elements include: an ACAS II interrogator-processing unit, ACAS antennas and a Mode S transponder.

The replies from the Mode S transponders are used to collect the following surveillance data:
The relative range. This is derived from the arrival time of the synchronised reply pulse, and is considered as an independent measure.
The relative bearing. This is derived from the antenna pattern, and is considered as an independent measure.
The altitude. This is derived by reading out the dependent altitude in the replies, based on altimeter navigation.

Despite the fact that ASAS and ACAS are largely independent by nature, they share some components (e.g. the traffic display). Alerts should be clearly distinguishable, so that the flight crews are aware of which system is providing the alert. If either ASAS or ACAS is tracking a target that is not tracked by the other system, the CDTI shows a target, and it is apparent which system has produced the target.

6. Human roles and tactical operations description

Human roles and responsibilities

The general responsibility of the aircrew is to carry out the mission of the aircraft in a safe and efficient manner. The responsibilities of the pilot-flying are focused around the correct implementation of aircraft manoeuvres; in particular
"nothing […] shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a conflict. " Pilots are trained to obey ASAS advisories. They are also trained to obey an ACAS RA even if ASAS gives an opposite instruction, even if the aircraft is close to the top of its operating envelope, even if the intruder cannot be seen at its indicated position or whatsoever. The responsibilities of the pilot-not-flying include the flightplan, communication and surveillance. Only aircraft with fully qualified crew have access to the FFAS. This implies that the crew is trained in keeping traffic situational awareness and preventing, identifying and resolving conflict situations, and in understanding and remembering ASAS equipment, CDTI symbology and CDR and Transition procedures."

The Pilot-Flying obtains situational awareness by monitoring the CDTI, other displays giving information on the aircraft systems, listening to the R/T and by looking out of the window. He executes aircraft manoeuvres via the auto-pilot or manually.

The Pilot-Non-Flying also obtains situational awareness by monitoring the CDTI, other displays giving information on the aircraft systems, listening to the R/T and by looking out of the window. He enters or deletes waypoints in the FMS, communicates with the pilot and with other crews by R/T and plays a role in emergency procedures.

ATC has the authority to give or refuse aircrew access into the FFAS.

Conflict Prevention

On the short term, the crew should not choose routes that are conflicting with other aircraft. An advisory module called P-ASAS warns for manoeuvres that may lead to short term conflicts, see paragraph "P-ASAS functionality" in Section 7.

Conflict Detection

The crew is responsible for detecting conflicts in the proper context. ASAS assists by alerting the crew in case of a conflict, giving additional information to increase the pilot's situational awareness.

We assume that the Protected Zone is based on separation minima, that are fixed. Only if the Actual Navigation Performance (ANP) achieved during flight has not the required accuracy, the numerical values for the separation minima are adapted.

The ASAS conflict detection module identifies potential intruders and predict their trajectory on the basis of the ADS-B information. The estimated the minimum distance at the closest point of approach (CPA) is compared with the required separation. A potential conflict is detected and presented by ASAS as such, if time to intrusion (the point in time where the separation minima are actually violated) is within the so-called look-ahead time. A typical look-ahead time is 5 minutes.

Conflict Resolution

Once a conflict is detected, it is the pilot's responsibility to take proper actions to avoid a loss of separation, taking into account the weather, the aircraft's current performance, the reliability of the information, etc. In case several conflicts are detected simultaneously, they are solved sequentially, according to the time to intrusion.

Two CR phases can be distinguished. In the first phase, called the priority rules based phase, one aircraft is assigned a "right of way", giving the aircraft's crew the freedom to manoeuvre although it is not mandatory. The other aircraft is required to make a manoeuvre that solves the conflict. Once the time to loss of separation becomes too small (goes below a 'threshold' value), then a second phase starts, called the co-operative phase, in which both aircraft are required to manoeuvre, in a co-operative way.

ASAS will determine the priority in the first phase of the conflict according to a set of rules. Each individual ASAS system determines who has the right-of-way and this is not acknowledged explicitly (except in open issue 3, see Section 4, where all aircraft involved in a conflict broadcast whether they have priority and check the received priority information). The priority is indicated on the CDTI's of the involved aircraft such that it is clear which aircraft will have to manoeuvre to solve the conflict.

ASAS generates Conflict Resolution options, leaving the pilot the following options:

- Choose a horizontal resolution by a heading change.
- Choose a vertical resolution by an altitude change.
- Choose a combination of a horizontal and a vertical resolution.
- Engage a manually determined solution.

The ASAS proposed Conflict Resolution options will be displayed on the CDTI. In an advanced setting, the ASAS might suggest a most-preferred CR manoeuver but it is the pilot who is in command, being able to take situational information into the decision. While choosing, the crew shall take into account additional constraints, e.g. SUA's, danger weather areas, terrain, etc.

The pilot must then execute the chosen resolution manoeuvre accordingly, while monitoring until the conflict has been solved. He can delegate this task to the ASAS, which has an interface to the auto-pilot. Finally, as part of the recovery action, ASAS indicates the moment and path of recovery, thus enabling the pilot to return to the originally intended path. The CDTI should enable crew to determine moment of recovery, i.e. when they can return to their original intended path. In case an aircraft cannot manoeuvre according to the ASAS proposals, the crew shall notify other aircraft in its vicinity of this.

In open issue 3 (see Section 4), after the aircraft which has to manoeuvre (the one not having priority) has decided how to resolve the conflict, its intention can be transmitted to the other aircraft (the one having priority). In this way the aircraft having priority may, if desired, execute a co-operative resolution manoeuvre safely without counteracting the manoeuvre of the other aircraft. This confirmation will be performed almost fully automatically by the ASAS via ADS-B. However, the crew may be more or less involved in this process (at least, aircrew should monitor the process), which imposes additional requirements to ASAS. After the pilot has decided how to resolve the conflict, the intended manoeuvre is transmitted to the other aircraft in order to resolve any singularities and in order to inform the other aircraft such that a co-operative manoeuvre can be chosen. In nominal situations both crews of aircraft involved in a conflict have exchanged information and do agree on:

- the phase of the conflict, whether it is priority rules based or co-operative,
- which aircraft has priority (during the priority rules based phase),
- which aircraft will make which CR manoeuvre.

7. Description of functionality

General overview

The figure below gives an impression of the relations between the main functionalities that play a role in the tactical operations, that is: in separation assurance and collision avoidance within the Free Flight concept. Within one aircraft, the following sets of functionalities can be identified: the aircraft systems (including the auto-pilot and the engines), the Flight Management System (that contains the Flight Plan and may execute it), the ASAS and surveillance functionality (as described in Section 5), the navigation (including the GPS receiver and the altimeters), ACAS (as described in Section 5), ADS-B (supporting digital communication) and R/T (supporting speech communication). The last three entities have intra-aircraft interaction, indicated by the arrows at the bottom of the figure pointing to functionalities of other aircraft that are not drawn (but have the same functionalities). Apart from the functionalities related to aircraft equipment, there are the global GPS system (including satelites) and the crew's roles.

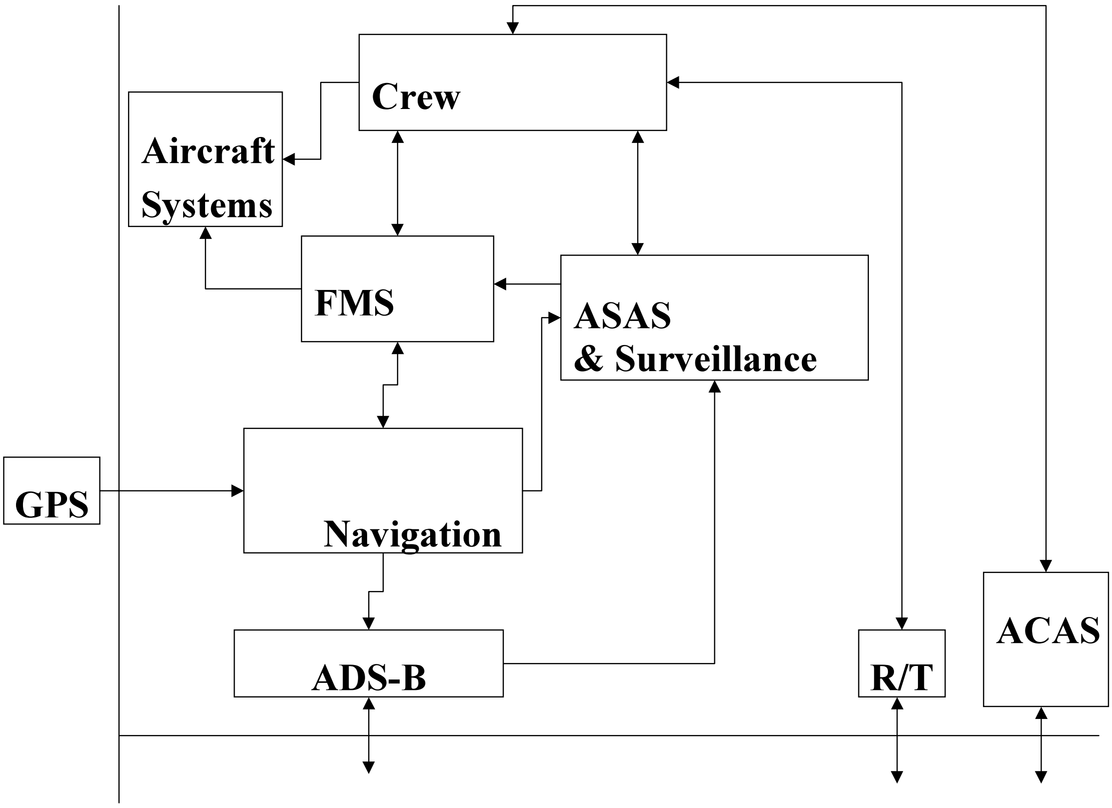

Figure 7.1 Impression of the relations between the main functionalities

Navigation

The GPS system sends out messages that are received by the individual GPS receivers, and that are processed by the individual navigation systems into an absolute horizontal position. This absolute horizontal position is expressed in a longitude and a lateral co-ordinate. The GNNS system and the individual GPS receivers have three modes: a) working in an incorrupt way b) working in a corrupt way without indicating this and c) unavailable. (If the system or receivers indicates that it is working in a corrupt way, is considered to be unavailable).

If the GNNS system or GPS receiver is unavailable, the INS system takes over the navigation and the navigation system also processes this in an absolute horizontal position, expressed in a longitude and a lateral co-ordinate. The individual INS systems have three modes: a) working in an incorrupt way b) working in a corrupt way without indicating this and c) unavailable. (If the system indicates that it is working in a corrupt way, is considered to be unavailable).

The altimeters measures the local pressure and the Navigation System translates this in a Flight level. The Flight level information is available or is not available.

The Navigation System deduces a horizontal velocity and a rate of climb, if the horizontal and vertical position information are available respectively.

The quality of the position and velocity information available in the individual Navigation Systems can be expressed by accuracy measures (that incorporate update rate, continuity, rounding off errors, etcetera).

ADS-B

The following information is broadcast by ADS-B transmitters and received by ADS-B receivers:

- The aircraft's call sign, corresponding to the one put in the FMS,
- Whether the aircraft is in emergency and is leaving the FFAS, where two different messages can be broadcast: requesting priority in conflict situation or indicating that all conflicts will be solved.
- The position and velocity information available in the Navigation System.

The ADS-B transmitters and receivers have two modes: a) working in an incorrupt way and b) unavailable. The horizontal range is limited; the vertical range is virtually not. There is a small cone of silence above and beneath each aircraft.

Surveillance processing and ASAS

Surveillance Processing

The own navigation data and the received dependent surveillance data are combined and processed to obtain:

- A relative horizontal position of other aircraft, expressed in a bearing and an angle.
- An absolute vertical position of all aircraft, expressed in a flight level.
- A relative horizontal velocity of other aircraft.
- A rate of climb of other aircraft.

P-ASAS functionality

On the basis of the surveillance information available, P-ASAS calculates which manoeuvres lead to a conflict. It indicates that it would lead to a conflict within the look-ahead time if the aircraft would now make an immediate heading or vertical speed change (leaving the other states like position and speed as they are). These manoevres are indicated by means of yellow and red bands on the CDTI, depending on the time to intrusion. As an implicit consequence, the lack of these P-ASAS bands indicate which manoeuvres can be made without potential conflicts. This function can also be used to revert from FMS coupled to basic auto-pilot modes without introducing a conflict. Moreover, if conflicts are detected, the conflict prevention tool prevents triggering new conflicts with other aircraft while making a conflict resolution manoeuvre.

Conflict detection, conflict alerting and priority determination functionality

The ASAS conflict detection module identifies potential intruders and predict their trajectory on the basis of the surveillance information. The estimated minimum distance at the closest point of approach (CPA) is compared with the required separation. A potential conflict is detected as such, if time to intrusion (the point in time where the separation minima are actually violated) is within five minutes.

The aircrew is immediately alerted, visually and aurally, and the CDTI informs the crew about the nature of the conflict: when (i.e. time to intrusion), where, who (i.e. identity of aircraft involved) and geometry of closest point of approach. If the potential conflict is not solved, a second alert goes off, indicating that the time to intrusion is now less than three minutes.

Conflict resolution advisory functionality

ASAS generates Conflict Resolution options according to an universal algorithm, i.e.: future manoeuvres that will resolve the current conflicts and, if possible, do not induce new conflicts, taking into account the aircraft’s performance. If possible, at least a horizontal resolution by a heading change and a vertical resolution by an altitude change are advised. In an advanced setting, the ASAS might suggest a most-preferred CR manoeuver.
It is assumed that all ASAS systems will use the same, universal CR algorithm with the property that the resulting motions of two aircraft that both make a CR manoeuvre will always be co-operative without any negotiation or communication required. The CR options are the same for the priority rules based phase and for the co-operative phase, and are the same for aircraft with and aircraft without the right of way.

If a conflict resolution manoeuvre turns out to induce an other conflict, it is rejected and not adviced. If all possible conflict resolution manoeuvres turn out to induce other conflicts, the one is chosen where the time to intrusion is the one most far away in time.

Whether the conflict resolution manoeuvre may or must be executed, depends on the phase of the conflict and the priority. During the first phase, one aircraft in one aircraft-aircraft encounter has priority according to a set of hierarchical rules:

- An aircraft in emergency has right of way over an aircraft that is not.
- An aircraft involved in two or more conflicts with incompatible priorities has right of way over an aircraft that is not.
- In a transition zone, an exiting aircraft has right of way over an entering aircraft.

- In a transition zone, an aircraft with a lower sequence number or earlier exit/entry time has right of way over an aircraft with a higher sequence number or later exit/entry time.
- An aircraft descending has right of way over an aircraft climbing.
- An aircraft with a low ground speed has right of way over an aircraft with a high ground speed.
- An aircraft far away from the CPA has right of way over an aircraft close to the CPA.
- In case none of the criteria determines priority, an arbitrary choice on e.g. the basis of the transponder address can be applied.

During the second phase, which starts if the time to intrusion is three minutes, no aircraft has right of way and both shall make an indicated conflict resolution manoeuvre.

ACAS

ACAS interrogation interval is typically once per second but can be speeded up or slowed down. The altitude reporting has a resolution of 25 ft, but only 100 ft in case of certain altitude coding transponders (compared to a standard 100ft for ground SSR replies).

In a nominal situation, ACAS thus tracks range, bearing, and altitude of each transponder equipped aircraft within cover, and might store aircraft identification. From this, the closure rate, the closure rate acceleration and the vertical speed for altitude reporting aircraft can be calculated. In addition, the data from own aircraft's pressure altimeter is taken into account, either directly from the altitude encoder or the ADC. Using this data, the relative altitude can be computed. A typical system can track at least 30 aircraft, up to 150, within a minimal 5 NM radius when operating in high density and within a 35 NM radius operating nominally.

For aircraft with a relative range and altitude within certain limits, a threat algorithm calculates the Closest Point of Approach (CPA) and the time to this CPA by means of extrapolation. If the CPA and the time to CPA are within certain limits a Traffic Advisory (TA) is given, which aims at helping the pilot in the visual search for the intruder aircraft, and by alerting him to be ready for a potential resolution advisory. A typical volume is a cylinder with a radius of 500 feet horizontally and a height of 400 feet. A TA occurs 15 to 48 seconds before the projected CPA. There is only one aural TA alert: "Traffic, traffic".

Depending on the variable protected volume, a RA is given from 15 to 35 seconds before the projected CPA. When both aircraft are ACAS equipped, co-ordination is achieved by a data exchange between the ACAS computers using in order to select complementary resolution senses. There are several types of aural RA message, as a corrective one ("Descend, descend"), a weakening one ("adjust vertical speed, adjust"), and one for reversing the sense of the vertical motion ("Climb, climb NOW").

If no ACAS alerts are given and if ASAS can relate ADS-B derived surveillance data with ACAS data, ACAS data is not shown on the CDTI. If an alert is given, the appropriate information is displayed on the CDTI:

- For which aircraft the alert is applicable,
- The position derived from ACAS data if it does not correspond to the ADS-B derived data,
- The proposed resolution manoeuvre in case of a RA.

HMI and CDTI

Before the ASAS and ACAS information are shown on the display, the information is processed in the following way:

- If both ASAS and ACAS information can identify one and the same target, and the positions according to both source correspond (according to a specific algorithm that takes into account the accuracy's), only the ASAS symbol is shown.
- If both ASAS and ACAS information can identify one and the same target, and the positions according to both source do not correspond, both the ASAS symbol and ACAS symbol are shown (including the standard available surveillance information).
- If only ASAS or ACAS can identify a target, only that symbol is shown (including the standard available surveillance information).

Two CDTI's are present in the cockpit, one for the pilot-flying and one for the pilot not-flying. Each display (and the related processing explained above) is available and works fine or is unavailable. The CDTI can display up to 100 aircraft at any one time.

8. Hazard identification

As the Free Flight concept is properly defined, and as the operational and physical boundaries of the operation under consideration are sufficiently specified in the previous chapter, a rather complete list of hazards can be identified. These hazards compromising safety may be failures of technical systems, problems with procedures, human errors etc. The identification of hazards can be achieved by means of brainstorm sessions, literature search and functional analysis. In [Everdij et al., 2002] a TOPAZ based collision risk study including bias and uncertainty assessment has been performed for flying with free flight equipped aircraft within a fixed route structure. This study identified and analysed some 300 hazards. These hazards also apply to the free flight operational concept considered in WP9. Additional hazards have been identified for the particular operation considered within WP9 [MFF-NLR, 2004].

All together this resulted in a list of in total more than 300 hazards. In order to get an idea of the individual hazards on this list, the table below specifies six examples of hazards from this list. These six examples form a nice illustration of the challenge that lies ahead of developing a Monte Carlo simulation model of the free flight operation considered.

Table 2. Hazard examples which challenge Monte Carlo simulation model development

1	Some aircraft symbols may not be seen well in sunlight, e.g., dark grey symbols.
2	Pilots making own judgement on relevance of (reported, alerted) failures or conflicts and acting only on alerts judged relevant; misjudgement may lead to not reacting to an important alert.
3	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.
4	Flight control related errors occur, possibly in combination with transponder problems. Especially smoke or rapid decompression.
5	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.
6	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.

References

[Abeloos] *Potential co-operations between the TCAS and the ASAS; A. Abeloos, M Mulder, R. van Paassen, E. Hoffman, International Conference on human-Computer Interactions in Aeronautics, Toulouse, Sept 2002*

[ARP 5365] *Aerospace Recommended Practice by Society of Automotive Engineers (The Engineering Society For Advancing Mobility Land Sea Air and Space), Human Interface Criteria for Cockpit Display of Traffic Information , 1999*

[Avermaete] *Evaluation of the traffic awareness questionnaire used at NLR, NLR TR 94206 L, J.A.G. van Avermaete, April 1994*

[Brooker] *Airborne Separation Assurance Systems: towards a work programme to prove safety, Peter Brokker, Safety Science, 42, pp 723-754, 2004*

[CARE/ASAS WP3] *Everdij , M.H.C., G.J. Bakker and H.A.P. Blom, CARE/ASAS Activity 3: Airborne Separation Minima – WP3 report: Estimating safe separations, Version 2.0, January 2002*

[DAG-TM] *Concept Defintion for Distributed Air/Ground Traffic Managemen (DAG-TM), version 1.0. Advanced Air Transportation Technologies Project, Aviation System Capacity Program, National Aeronautics and Space administration, NASA, 1999*

[D2.2] *Stochastic analysis background of accident risk assessment in Air Traffic Management, by H.A.P. Blom, G.J. Bakker, M.H.C. Everdij and M.N.J. van der Park, Final version, July 2003 (http://www.nlr.nl/public/hosted-sites/hybridge/)*

[D2.4] *Modelling hybrid state Markov processes through Dynamically and Stochastically Coloured Petri Nets, by M.H.C. Everdij and H.A.P. Blom, Draft 0.5, August 2003*

[D4.2] *CPDP: a compositional framework for stochastic hybrid systems of the PDP type by S.N. Strubbe and A.J. van der Schaft, Draft version 0.4, February 2004*

[D5.1] *Hierarchical Decomposition of Conflict Resolution Tasks, A. Lecchini and J. Lygeros, Draft, January 2004*

[D6.2] *Intermediate report on decentralized conflict resolution algorithms, Draft version 0.2, January 2004*

[D7.3] *Situational awareness error detection, by M. D. Di Benedetto, S. Di Gennaro, A. D'Innocenzo, Second draft, January 2004*

[D 8.3] *Monte Carlo simulation of rare events in hybrid systems by J. Krystul and H.A.P. Blom, Draft version 0.4, March 2004*

[Everdij et al, 2002] *Everdij, M.H.C., Bakker, G.J., Blom, H.A.P., Bias and uncertainty in accident risk assessment of an Extended Free Flight operational concept, NLR-TR-2002-691*

[FFlit] *Free Flight Research Issues and Literature Search, Under NASAS Contract NAS2-98005, J. Krozel, 2000.*

[Hawkes] *ACAS II, D Hawkes, JAA CNS/ATM Steering Group Position Paper pp017_12, 1998*

[Hoekstra] *Designing for Safety, the Free Flight Air Traffic Management concept, J. Hoekstra, thesis, Nov 2001*

[Hybridge Project]	*Hybridge Project Management Plan, WP 0, Version 0.2, HYBRIDGE/NLR/WP0/PMP/0.2, March 2002*
[ICAO ASAS Circ]	*ICAO Draft Airborne Separation Assistance System (ASAS) circular, Version 3.0., SCRSP, WGW/1, WP/5.0,2003*
[ICAO Data Link application]	*ICAO Manual of Air Traffic Services Data Link Applications, Doc 9694, 2001*
[MFF Briefing]	*Mediteranean Free Flight Briefing guide, February 2004, Verion 1.0, Ed. R. Ruigrok*
[MFF-NLR, 2004]	*MFF Free Flight experiments 2004, NLR team, working document, to be published*
[MOPS ASSAS]	*Minimum Operational Performance Standards for Airborne Surveillance and Separation Assurance Processing (ASSAP). RTCA SC186 WG4. Draft 0.6. March, 1999.*
[MOPS CDTI]	*Minimum Operational Performance Standards for Cockpit Display of Traffic Information. RTCA SC 186. Version 25-v2. November, 1999.*
[OCD]	*Operational Concept Document . EUROCONTROL. FCO.ET1.ST07.DEL01. Edition 1.1. January, 1999*
[PO-ASAS]	*Principles of Operations for the Use of ASAS, Action Plan 1 FAA/Eurocontrol Cooperative R&D, Version 7.1, 2001.*
[RTCA CO CM]	*Concept of Operations for Airborne Conflict Management: Detection, Prediction and Resolution, RTCA SC-186 WG1, May 25, 2000.*
[SAF-ASAS]	*Safety And ASAS applications, Action Plan 1 FAA/Eurocontrol Cooperative R&D, Version 4.1, 2004.*
[SRC 2]	*SRC Policy Document 2, Use of safety nets in Risk Assessment & Mitigation in ATM, edition 1.0, April 2003*

Abbreviations

ACAS	Airborne Collision Avoidance System
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance-Broadcast
ANP	Available/Estimated Navigation Performance
AOC	Air Operator Certificate
ASAS	Airborne Separation Assurance System
ASOR	Allocation of Safety Objectives and Requirements
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
CD	Conflict Detection
CDR	Conflict Detection and Resolution
CDTI	Cockpit Display of Traffic Information
CNS	Communication, Navigation, Surveillance
DME	Distance Measuring Equipment
FAR	Federal Aviation Administration
FFAS	Free Flight Airspace
FIR	Flight Information Region
FMS	Flight Management System
FIR	Flight Information Region
FLOS	Flight Level Orientation Scheme
ft	Feet
GNE	Gross Navigation Error
ICAO	International Civil Aviation Organisation
INS	Inertial Navigation System
JAA	Joint Aviation Authority
MAS	Managed Airspace
MFF	Mediterranean Free Flight
ND	Navigation Display
NDB	Non-Directional Beacon
Nm	Nautical miles
OHA	Operational Hazard Analysis
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
P-ASAS	Preventive ASAS
PF	Pilot-flying
PFD	Primary Flight Display
PNF	Pilot-not-flying
RA	Resolution advisory
RCP	Required Communication Performance
RNP	Required Navigation Performance
RSP	Required Surveillance Performance
RVSM	Reduced Vertical Separation Minima
SARPS	Standards and recommended Practices
SSR	Secondary Surveillance Radar
SUA	Special User Airspace

TA	Traffic Advisory
TCAS	Traffic alert and Collision Avoidance System
TIS-B	Traffic Information Service-Broadcast
TMA	Terminal Manoeuvring Area
TMS	Technical Management System
TOD	Top Of Descent
TOPAZ	Traffic OrganiZation and Perturbation AnalyZer
UMAS	Unmanaged Airspace
VDLM4	Very High Frequency Data Link Mode 4
VOR	VHF Omni-directional Range