Making change in En-Route Air Traffic control

DELIVERABLE

EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

FIRST ATC SUPPORT TOOLS IMPLEMENTATION PROGRAMME

EUROCONTROL

EUROCONTROL DAS/ATS

FASTI Preliminary Safety Case

Edition Number	**:**	**1.0**
Edition Date	**:**	**14 May 2008**
Status	**:**	**Proposed Issue**
Intended for	**:**	**FASTI Steering Group**

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
FASTI Preliminary Safety Case		
	EATMP Infocentre Reference:	
Document Identifier	**Edition Number:**	1.0
	Edition Date:	14/05/08

Abstract

The First ATC Support Tools Implementation (FASTI) Programme aims to offer improvements in safety, capacity and efficiency by implementing new automated tools to support controllers in conflict detection, planning, monitoring and co-ordination. EUROCONTROL's role is to co-ordinate, harmonise and expedite the implementation of these tools. ANSPs, supported by industry, will be responsible for implementation and operation.

This document is a Preliminary Safety Case (PSC) for the FASTI tools and their associated human and procedural elements. It comprises a structured Argument and Evidence, showing that the FASTI concepts and high-level design as proposed by EUROCONTROL can be made acceptably safe for use in the proposed operational context.

A number of Safety Issues remain to be addressed before this claim can be fully substantiated and the PSC finalised. The main needs are to ensure that adequate ANSP input is obtained, and that appropriate simulations are carried out.

Full Safety Cases, demonstrating operational safety, and providing a basis for licensing and auditing by national safety regulators, will need to be developed by the implementing ANSPs in parallel with their detailed design and implementation of operational systems, taking account of their specific operational contexts and needs.

This PSC identifies key areas in which ANSPs will need to review or develop the Arguments and Evidence in parallel with their evolving designs and plans for implementation. More detail of how to do this is provided in a separate Guidance document.

Keywords

Safety	Safety Case	Safety Study	Safety Assessment
Safety Argument	Human Factors	Cognitive Task Analysis	FHA/ PSSA
Conflict	Resolution	Planning Controller	Tactical Controller
Hazards	Computer assistance	En-route	

Contact Person(s)	Tel	Unit
Predrag Terzioski	(32) 2 729 3347	DAS/ATS
David Nicholls	(44) 1235 555755	RM Consultants Ltd

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	☑	General Public	☐	Intranet	☐
Draft	☑	EATMP Stakeholders	☐	Extranet	☐
Proposed Issue	☐	Restricted Audience	☑	Internet (www.eurocontrol.int)	☐
Released Issue	☐	*Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)*			

ELECTRONIC SOURCE		
Path:		
Host System	Software	Size
Windows_NT	Microsoft Word	Kb

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Please make sure that the EATMP Infocentre Reference is present on page ii.		
Consultant Team Authors	Editing author: David Nicholls - RM Consultants Ltd (Consultant Team Project Manager) Contributors: Toni Close & David Jamieson - BOMEL	14/05/08
EUROCONTROL Project Manager		

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	12/11/07		First Draft	All
0.2	26/03/08		Comments from FASTI team	All
1.0	14/05/08		Further comments from FASTI team	All

CONTENTS

EXECUTIVE SUMMARY

The First ATC Support Tools Implementation (FASTI) programme is being developed by EUROCONTROL together with Air Navigation Service Providers (ANSPs) and industry representatives. The aim of the programme is to offer improvements in safety, capacity and efficiency by implementing new automated tools to support controllers in their tasks of conflict detection, planning, monitoring and co-ordination. FASTI should result in a shift from sector-focussed, tactical and reactive operational behaviour to trajectory-oriented, strategically-planned, conflict-free behaviour.

EUROCONTROL's role is to co-ordinate, harmonise and expedite the uptake of the FASTI system. ANSPs, supported by industry, will be responsible for the actual implementation of operational systems.

In order to comply with EUROCONTROL policies and meet the wider safety aspirations of the aviation community, it is necessary to carry out a thorough and systematic safety assessment before implementing any significant changes to ATM systems. In particular, the safety of any significant new system (in this case the FASTI tools and their associated human and procedural elements) needs to be assured by the development of a series of Safety Cases accompanying the progression through the lifecycle.

This document is EUROCONTROL's Preliminary Safety Case (PSC) for the concept and high-level design of FASTI as proposed by EUROCONTROL.

The technical core of the PSC is a Safety Argument: a systematic, hierarchical presentation of the Arguments, substantiated by Evidence, that supports the top-level Claim that the concept and high-level design will be acceptably safe for operational use. The Safety Argument provides a structured, informed basis for discussing safety with stakeholders, and a starting point for ANSPs to develop, update or benchmark their own Safety Cases.

With regard to the overall Claim that FASTI will be safe for operational use, this PSC has shown that the FASTI concept and high-level design can satisfy this claim in the proposed operational context.

A number of Safety Issues remain to be addressed before this claim can be fully substantiated and the PSC finalised, but none of these are seen as being particularly difficult to resolve in principle. The main needs for the future are to ensure that adequate ANSP input is obtained, and that appropriate simulations are carried out.

The next stage will be for each ANSP to undertake more detailed definition and design, taking account of their specific operational context and needs, and to plan for implementation, transition and operation. It will be for each ANSP and their national regulators to determine, within the context of overall European and EUROCONTROL requirements, how to optimise the balance between the potential safety, operational and efficiency benefits of FASTI. In parallel with this, ANSPs will need to develop the PSC into a full Safety Case, demonstrating operational safety, and providing a basis for licensing and auditing by national safety regulators.

The main output of the PSC that will be important to implementing ANSPs is the set of Safety Requirements. These are requirements on the ongoing functionality, performance, reliability or integrity of the operational system, which each ANSP will need to ensure are satisfied.

This PSC also contains outline Guidance to ANSPs, identifying key areas in which they will need to review or develop the Arguments and Evidence in p arallel with their evolving detailed design and plans for implementation. More detail of how to do this is provided in the separate Guidance document [Ref.1]

1. INTRODUCTION

1.1 Background

The First ATC Support Tools Implementation (FASTI) programme is being developed by EUROCONTROL together with Air Navigation Service Providers (ANSPs) within the European Civil Aviation Conference (ECAC) States and industry representatives. The aim of the programme is to offer improvements in safety, capacity and efficiency by implementing new automated support tools for controllers in their tasks of conflict detection, planning, monitoring and co-ordination.

More specifically, FASTI has the following aims:

- to increase sector capacity, improve flow rates, and reduce delays;
- to increase the potential for flexibility, changes in operational practices and changes in conditions specified in Letters of Agreement (LOAs);
- to introduce the potential for cost savings through the automation of routine tasks, flexible staffing and future system and airspace development; and
- to support an improved quality of service to airspace users in the form of optimum profiles and routes, and less ATC intervention.

EUROCONTROL's role is to co-ordinate, harmonise and expedite the implementation and operation of these tools. ANSPs, supported by industry, will be responsible for the actual implementation and operation.

In order to comply with EUROCONTROL policies and meet the wider safety aspirations of the aviation community, it is necessary to carry out a thorough and systematic safety assessment before implementing any significant changes to ATM systems. The safety of the new system needs to be demonstrated in a full Safety Case. The present Preliminary Safety Case (PSC) is the first step towards this.

1.2 Aim of the Preliminary Safety Case

The aim of this PSC is to demonstrate, as far as possible at this stage, that the FASTI System as proposed by EUROCONTROL will be safe in operational service.

1.3 Purpose - why and for whom the document is written

The PSC is written to give EUROCONTROL assurance that what is being promoted in the FASTI Programme is acceptably safe. It also provides the EUROCONTROL FASTI Project Team with an informed basis for managing safety effectively in the ongoing development and demonstration of the FASTI tools.

In addition to its uses within EUROCONTROL, the PSC is intended to provide a readily adaptable model that ANSPs can use to develop, benchmark or update their own Safety Cases for operational systems.

This PSC is therefore accompanied by a separate Guidance document [Ref.1], providing further support for ANSPs.

1.4 Scope

1.4.1 Components of the FASTI system

All elements of the FASTI system, i.e. the People, Procedures and Equipment (hardware and software) associated with the tools, are considered. The tools currently included in the FASTI Programme are:

Medium Term Conflict Detection (MTCD)

MTCD enhances planning by facilitating early detection of conflicts. It is thus an additional safety barrier and facilitates more flexible routing. Specifically, it assists the controller in conflict identification and planning tasks by:

- providing automated early detection of potential conflicts;
- facilitating identification of flexible routing/conflict free trajectories;
- Identifying aircraft constraining the resolution of a conflict or occupying a flight level requested by another aircraft.

Monitoring Aids (MONA)

MONA helps controllers reduce the workload associated with routine traffic monitoring tasks by:

- providing warnings if aircraft deviate from a flight plan or clearance;
- providing reminders of instructions to be issued (e.g. to transfer an aircraft as it approaches the boundary); and
- triggering the trajectory re-calculation that is essential for MTCD.

System Supported Co-ordination (SYSCO)

SYSCO supports co-ordination between Planner Controllers (PCs) in different sectors or centres by facilitating screen-to-screen exchange of information, thus reducing the workload associated with telephone-based co-ordination. It includes the message set, the HMI and procedures for their use. SYSCO facilitates earlier resolution of conflicts, improves controller situational awareness and can enable new operational concepts such as MTCD planning. Coordination is performed automatically on the basis of sector boundary conditions contained in the trajectory. FASTI will provide procedures and guidelines for effective, uniform use of this automation across sectors and centres, resulting in more silent coordination.

The PSC argument structure has been designed (*inter alia*) to facilitate inclusion of other tools in future if required. For example, one such tool, currently being developed by EUROCONTROL, may be Tactical Controller Tools (TCT), which provides tactical conflict identification and resolution advice for the Tactical Controller. The PSC allows for such additions by focussing on high level concepts and functions and on the

generic issues that can arise when developing and implementing new automated systems rather on than the details of specific tools.

1.4.2 Allowing for different implementations of FASTI

FASTI has been defined such that it could, in principle, be implemented in any European en-route airspace where traffic is under radar control, while recognising that there will be differences in the way that individual ANSPs will implement it. For example:

- the three tools (MTCD, MONA and SYSCO) are considered as a package, but some ANSPs may wish to implement only part of the package;
- local differences in operational context (traffic levels, airspace structure etc) may affect the way that the tools are implemented and used. For example, FASTI may be implemented with different degrees of delegation from human to automation. MONA for example, may be implemented to detect a limited or more extensive range of non-conformances;
- ANSPs will assign differing priorities to the needs to improve safety, capacity or efficiency; and
- ANSPs will start from different points: some will already have the necessary enablers for FASTI in place, others will have to implement them (and demonstrate their safety) first. Some ANSPs already have FASTI-like tools in operation.

The PSC is designed to be applicable across variations such as these. The Guidance [Ref.1] will help ANSPs adapt and extend this generic model for their specific situations, by highlighting the differences that may arise and how they may be addressed.

1.4.3 Lifecycle Stages

Figure 1 shows how the lifecycle has been conceptualised for the present purpose, and how the responsibilities of EUROCONTROL and the ANSPs are divided between the lifecycle stages. Note that, while EUROCONTROL is performing the Definition stage, ANSPs will, as a minimum, need to review the validity of the Definition in relation to their own needs and context.

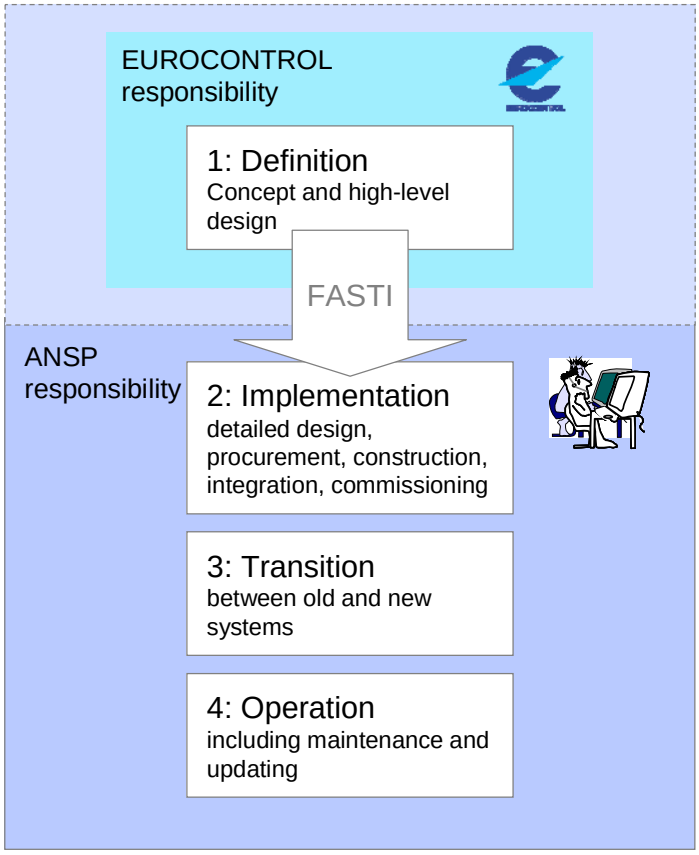

Figure 1: FASTI Lifecycle Stages - EUROCONTROL and ANSP responsibilities

This PSC is principally concerned with EUROCONTROL's responsibilities for the Definition of the system (Stage 1 in the Figure above). It also contains outline Arguments for the later stages of the lifecycle (2, 3 and 4), in order to provide confidence that it will be feasible for ANSPs to ensure safety – i.e. that the definition does not imply unreasonable expectations of what ANSPs can achieve.

Each ANSP will need to take account of its specific needs and operational context, and, by developing a full Safety Case, or by other means, assure themselves of safety in operation, and demonstrate this to their national safety regulators. For ANSPs, the PSC (in conjunction with the Guidance document) provides a starting point that can be extended to cover all stages of the lifecycle. In this way, the PSC aims to facilitate the handover of safety matters from EUROCONTROL to ANSPs.

While EUROCONTROL encourages harmonised implementations of FASTI and approaches to safety assessment wherever possible. However, ANSPs must not assume that all of the material presented here can be applied to their specific needs or operational environment.

1.4.4 Level of detail

The Definition stage shown in Figure 1 includes the overall concept and high-level design of FASTI. 'High-level' means that the PSC considers the basic building blocks of the system: the controller, the various

automated tools, the HMI and the external ATM systems that interface with FASTI, and the flows of information between them. This level of detail may be more familiar to some readers as a 'conceptual design'.

The high-level design does not specify details such as the internal architecture of these building blocks or the formats and protocols for data processing and transfer. However, because the FASTI Definition is still evolving, the boundary between EUROCONTROL's high-level design, and implementation-specific, detailed design issues for ANSPs, is somewhat fluid. Also, the new tools within FASTI are at varying states of development, with variable levels of information available for safety assessment.

The approach taken in the PSC has been to take a common, high-level view of the FASTI system, in order to provide a balanced picture, rather than including all the detail available.

The resulting, somewhat arbitrary, division between 'high-level' and 'detailed' design should not affect the validity of the eventual operational Safety Cases, because ANSPs will need to review (as a minimum) the generic concept and high-level design as well as considering the safety of their own detailed design work. In a full Safety Case, the boundary between high-level and detailed design will be dissolved.

1.4.5 Status of the current version of the PSC

This version of the PSC has been developed with input from the FASTI project team, which includes operational experience, and from a workshop with regulators and industry.

Each ANSP will have different priorities in implementing FASTI and will be at different stages of the process. Operational contexts vary, as do existing approaches to safety assessment, management and regulation. Input from individual ANSPs has so far been obtained in *ad hoc* contacts, but it is planned to make further, more focussed, contact with ANSPs. This will identify more fully and systematically the range of needs, constraints and expectations amongst ANSPs, and hence refine the present PSC and Guidance to be more helpful to them.

The PSC is a living document, and it is intended that it will be further refined through safety team participation in the FASTI simulations that are to be conducted at the EUROCONTROL Experimental Centre (EEC). The aim will be to ensure that the design and conduct of the simulations enables safety matters to be investigated as fully as possible, and to use the results to provide arguments and evidence for the PSC.

1.5 Overview of the method and outputs of the PSC

The PSC has been developed in accordance with EUROCONTROL good-practice guidance. It follows the safety assessment and management processes set out in the Safety Case Development Manual (SCDM) [Ref.2], the Safety Assessment Methodology (SAM) [Ref.3] and the EUROCONTROL Safety Regulatory Requirement on Risk Assessment and Mitigation in ATM (ESARR4) [Ref.4].

The technical core of the PSC is a Safety Argument: a systematic, hierarchical presentation of the Arguments, substantiated by Evidence,

that support the top-level Claim that the system will be acceptably safe for operational use. The Safety Argument provides a structured, informed basis for discussing safety with stakeholders, and a starting point. for ANSPs to develop, update or benchmark their own Safety Cases.

Where (within the scope of EUROCONTROL's responsibility) the Arguments and/ or Evidence cannot yet be fully developed, Safety Issues are raised and Safety Recommendations are proposed by which EUROCONTROL could address them in future.

A more specific output of the PSC, of particular importance to ANSPs, is the set of Safety Requirements. These are requirements on the ongoing functionality, performance, reliability or integrity of the operational system, which each ANSP will need to ensure are satisfied.

This PSC also contains outline Guidance to ANSPs, identifying key areas in which they will need to review or develop the arguments and evidence. ANSPs will need to review *all* of the PSC thoroughly and develop or adapt it where necessary. Guidance is only shown explicitly where it is important to draw attention to some specific aspect that will need to be reviewed, or suggest a particular way of doing so. Further supporting material for ANSPs is provided in the separate Guidance document [Ref.1].

1.6 Structure of the PSC

Section 2 describes the proposed FASTI system.

Section 3 introduces the high level structure of the Safety Argument (it is divided into four main Arguments reflecting the lifecycle stages of Definition, Implementation, Transition and Operation).

Section 4 gives a more detailed breakdown of the Arguments for lifecycle stage 1 (Definition) with supporting Evidence.

Section 5 provides outline Argument structures for lifecycle stages 2 to 4, i.e. those Arguments ANSPs will need to develop further. Evidence cannot yet be provided for these stages.

Section 6 summarises the assumptions and outstanding issues in the present PSC, and any limitations on the operation of FASTI that are currently apparent

Section 7 provides the conclusions of the PSC at this stage.

2. SYSTEM DESCRIPTION

FASTI aims to offer improvements in safety, capacity and efficiency by supporting controllers in their tasks of conflict detection, planning, monitoring and co-ordination. The key document for an overview of FASTI is the Operational Concept [Ref.5].

General descriptions of the three main component tools are available in

- for MTCD: the MTCD Concept of Operations [Ref 6], Operational Service and Environment Description (OSED) [Ref 7] and Operational Requirements and Implementation Guidelines [Ref 8]
- for MONA; the MONA OSED [Ref 9].
- for SYSCO: the CORT Implementation Strategy [Ref 10] The key reference for Trajectory Prediction (TP), which supports and interacts with the main tools, is the TP Operational Requirement [Ref 11].

This section summarises relevant information from these documents in order to provide a general awareness of the FASTI concept and high-level design, sufficient to understand the PSC.

FASTI is not a stand-alone system, but a set of changes to the existing ATM system, which will be integrated with the existing system. We have therefore defined FASTI in terms of the changes to the existing system (and will compare its safety against that of the existing system).

Because pre-FASTI situations will vary across ANSPs and States, we need to define (to the extent and detail necessary) a 'typical' baseline pre-FASTI situation. The chosen baseline is summarised below, with further details in Appendix C.

The Assumed Pre-FASTI baseline

- TC/PC working as a pair for each sector
- FDPS
- OLDI v3 and the basic messages for co-ordination and transfer

If an ANSP starts from a different baseline, they will need to adapt and develop their Safety Case accordingly. For example, if an ANSP needs to implement some enabling measures to come up to the baseline, they would need a Safety Case covering the implementation of enablers as well as implementation of the changes from baseline to FASTI.

Because ATM is a complex system with many dependencies and feedbacks, it is not possible to show it, or the changes that will result from FASTI, in any single picture of the system, without excessive repetition and complex detail. Three different views of the system are given in order to ensure a more complete identification of changes, as follows:

- a **Barrier Model** (Section 2.1), showing the barriers that ATM provides against accidents;

- an abstract **Functional Model** of ATM (Section 2.2). Although this is unchanged by FASTI, the performance of some functions will be improved, and some will be relied upon to greater or lesser extent. This Model also describes the functionality that the Logical Model (see below) will have to deliver; and
- a **Logical Model** (Section 2.3) showing the high level-design of the system – the allocation of the functions to an architecture of people, procedural and equipment elements

Key features of the overall picture that emerges from these three views are described in Section 2.4.

2.1 ATM Barrier Model

Figure 2 shows a generic model, developed from that in ICAO Doc 9854 [Ref.12] of how ATM contributes to the safety of aviation by providing a series of barriers to the hazards inherent in the existence of air traffic.

Since FASTI is intended for en-route application, the main (but not the only) types of incident and accident of concern are infringements of separation and mid-air collisions between aircraft.

The inputs to the model are the factors that determine the level of risk that would exist in the absence of ATM are principally the volume and pattern of traffic. These, *inter alia,* will determine the demands on and subsequent behaviour of the barriers.

For simplicity, the barriers are shown as mutually independent, operating from left to right in a rough time sequence, with each barrier contributing to safety by removing a proportion of potential conflicts. In reality their operation may interact and overlap in time. Common cause failures may cause the "holes" in each barrier to be aligned - inputting an incorrect Cleared Flight Level, for example, might cause a failure in the Conflict Avoidance, ATC Tactical Deconfliction and ATC Recovery barriers. The model is a way of looking at the generally available safety barriers, rather than a 'working' model of the actual barriers operating in any particular situation.

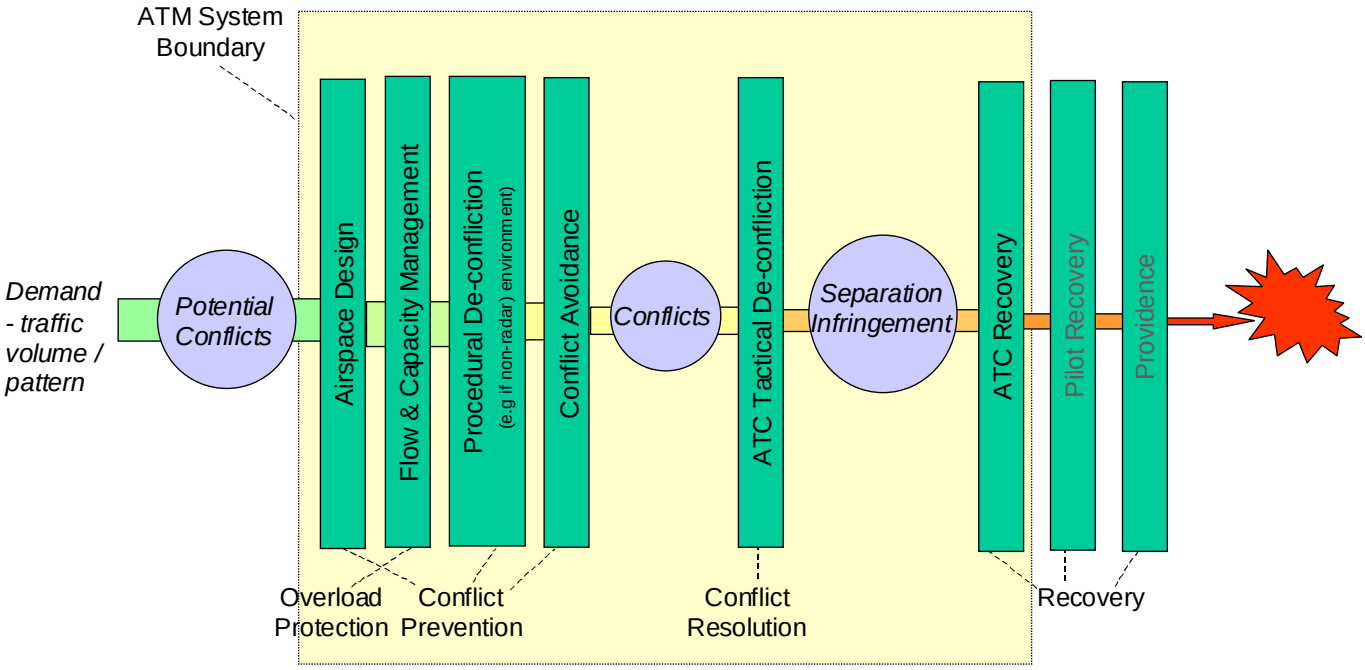

Figure 2 – ATM Barrier Model

- *Airspace Design* structures the airspace to keep aircraft apart spatially, in the lateral and/or vertical dimensions;
- *Flow and Capacity Management* mainly prevent overload of the *Separation Provision* barriers, by restricting, where necessary, the numbers of aircraft entering the airspace
- *Procedural Deconfliction* provides for separation of traffic in, for example, non-radar airspace;
- *Conflict Avoidance* involves planning the routing and timing of individual flights so that aircraft, if they followed their planned trajectories, will pass each other with at least the prescribed minimum separation. This barrier is in effect an abstraction of the role of the PC and also includes associated procedures such as those for co-ordination and transfer (CORT), LOAs etc
- *ATC Tactical Deconfliction* involves detecting conflicts when they occur and resolving the situation by changing the heading, altitude or speed of the aircraft appropriately. This barrier is in effect an abstraction of the role of the Tactical (or Executive) Controller (TC) and associated procedures.
- *ATC Recovery* represents “late” intervention by ATC, triggered, typically, by STCA (when implemented as a safety net);
- *Pilot Recovery* represents intervention by the pilot triggered, typically, by an ACAS RA; and

- *Providence* is the chance that, given the geometry of the specific encounter the aircraft, although in close proximity and below separation minima, would not actually collide.

None of the barriers is 100% effective even when working to full specification. The extent to which the barriers are able to reduce risk depends primarily on the functionality and performance of the various elements of the ATM system that underlie each barrier. If a barrier fails, risk will increase, either because that barrier is ineffective and/or because a new source of risk is induced by the failure.

Effects of FASTI on the Barrier Model

In terms of the Barrier Model, the main difference between FASTI and current (baseline) systems is that, by supporting the controllers' planning functions of monitoring and co-ordination, FASTI enables the Conflict Avoidance barrier to be strengthened.

FASTI does not in itself weaken other barriers, but could enable improved efficiency or flexibility of the ATM service by, for example, allowing more direct routeing of aircraft and removing some constraints on ATC practices Some examples, based on those in the Op Con [Ref.5] are noted below:

- reduction in the use of Flight Level Allocation Systems – use of semi-circular allocation and progression to the tactical use of "all levels";
- reduced constraints: changes to standing agreements, based on procedural separations, by lifting the need for ATC constraints related to airspace and sector organization;
- reduced level capping: more tactical allocation of cruising levels due to enhance planning, conflict detection and co-ordination;
- enhanced flexibility or efficiency of civil/ military coordination procedures;
- changes to co-ordination LOAs such as reductions in longitudinal separation planning minima between ATSUs. Changes to radar handover procedures in order to improve flexibility; and
- migration from the use of heading to track when radar vectoring, hence avoiding the current inconsistency between ground and airborne systems.

2.2 Functional Model

Figure 3 shows an abstract functional representation of the ATM Service (i.e. showing what the Service does, but not what system elements provide those functions), as applicable to an en-route environment.

The primary function of en-route ATM is to maintain the required separation minima between individual aircraft and between aircraft and restricted airspace.

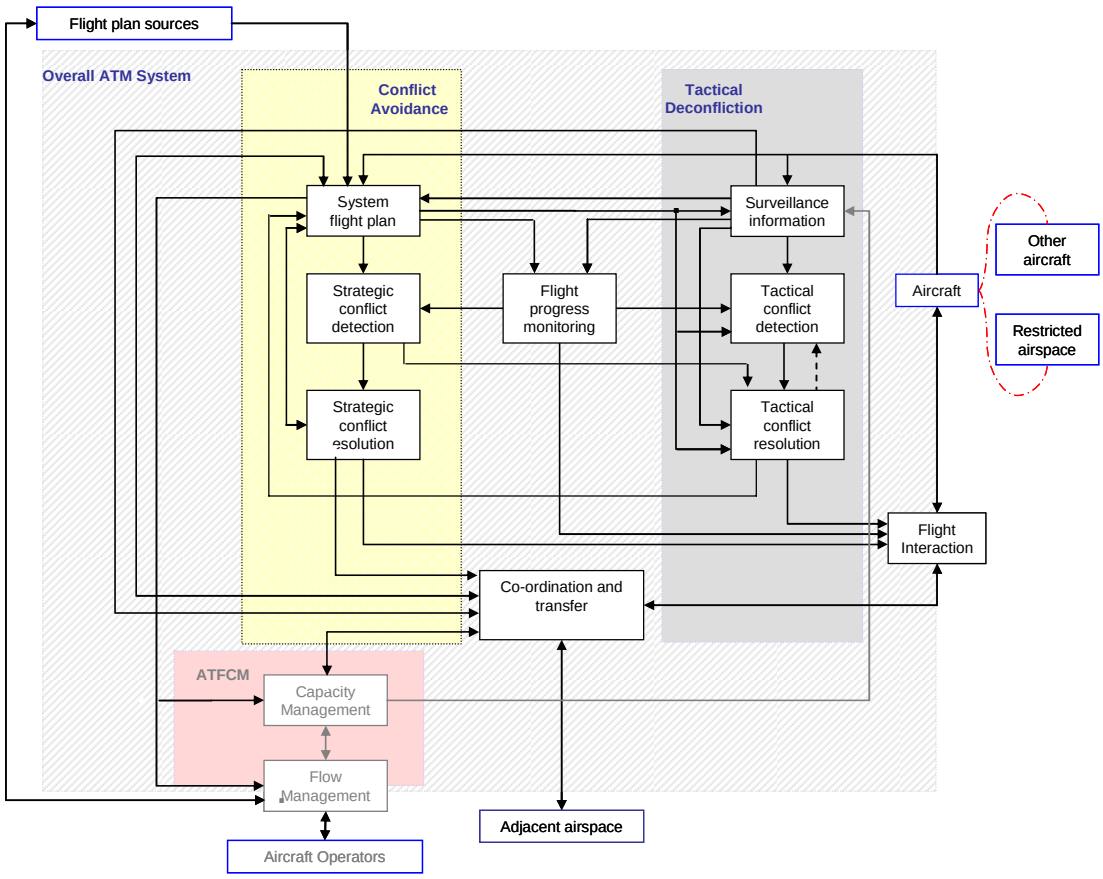

Figure 3 –ATM Functional Model for FASTI

Progressively updated (strategic) information concerning the flight is exchanged by the Coordination and Transfer (CORT) function before the flight is planned to enter the airspace concerned. Prior to the planned entry into the airspace, the flight details are checked by the Strategic Conflict Detection (SCD) function for conflicts.

If there is a conflict, it is resolved either by

- the strategic conflict resolution (SCR) function, resulting in a request to the handing-over control authority, via the CORT function, to modify to the aircraft's trajectory; or
- slightly later, tactically, as below.

When appropriate, the aircraft's flight data are updated by the System Flight Plan(ning) (SFP) function.

Prior to the aircraft entering (and eventually exiting) the airspace, the coordination and transfer function effects the handover of control responsibility from the previous control authority.

Short-term separation is maintained by Tactical Deconfliction using surveillance (and flight plan) information to detect and resolve conflicts and pass the resulting instructions and clearances via the flight interaction function.

The primary objective of Conflict Avoidance is to detect, and where appropriate remove conflicts before Tactical Deconfliction, thus reducing

the workload on the latter and reducing the risk of a conflict remaining undetected.

Flight Progress Monitoring (FPM) checks conformance between actual and cleared trajectories, and resolves any non-conformance through tactical conflict resolution / flight interactions and, where appropriate, an update to the system flight plan.

The Capacity Management (CM) function ensures (strategically) that the traffic capacity is matched to the expected pattern of short-term traffic demand economically, but without impairing the safe, orderly, and expeditious flow of traffic. Flow Management (FM) ensures that the traffic capacity and traffic demand are balanced tactically, such that overload of the other ATM capabilities does not exceed the declared capacity of the ATM service (for the current configuration).

Effect of FASTI on the Functional Model

The abstract functions of ATM are unaffected by FASTI. The purpose of FASTI is to provide automated support for the controllers' tasks of conflict detection, planning, monitoring and co-ordination, not to change them fundamentally.

Although the functionality is not changed, the performance of SCD, SCR, FPM and CORT will be improved. Also, FASTI will place greater demands on System Flight Planning, in that it relies on flight plan data being accurate and up-to-date. There will probably be fewer demands on Flight Interaction, since the more pro-active approach to control should require fewer tactical interventions. It may also facilitate FM and CM.

2.3 Logical Model

The Logical Model (Figure 4) represents the high-level design of FASTI as an architecture of physical building blocks or actors in the ATM system, both machine and human based, that are relevant to an operational FASTI system.

In order to keep this high level model as widely applicable as possible, all controller roles, PC and TC, are shown together in the 'Controller' box rather than being separated. This allows for the fact that some aspects of the division of roles may vary between different implementations of FASTI. For example in some cases MTCD may be a tool for the PC only, in others the TC may also be able to use it. It also allows the same model to represent cases such as single-person operation, as well as the more usual PC/ TC pairing assumed in the baseline.

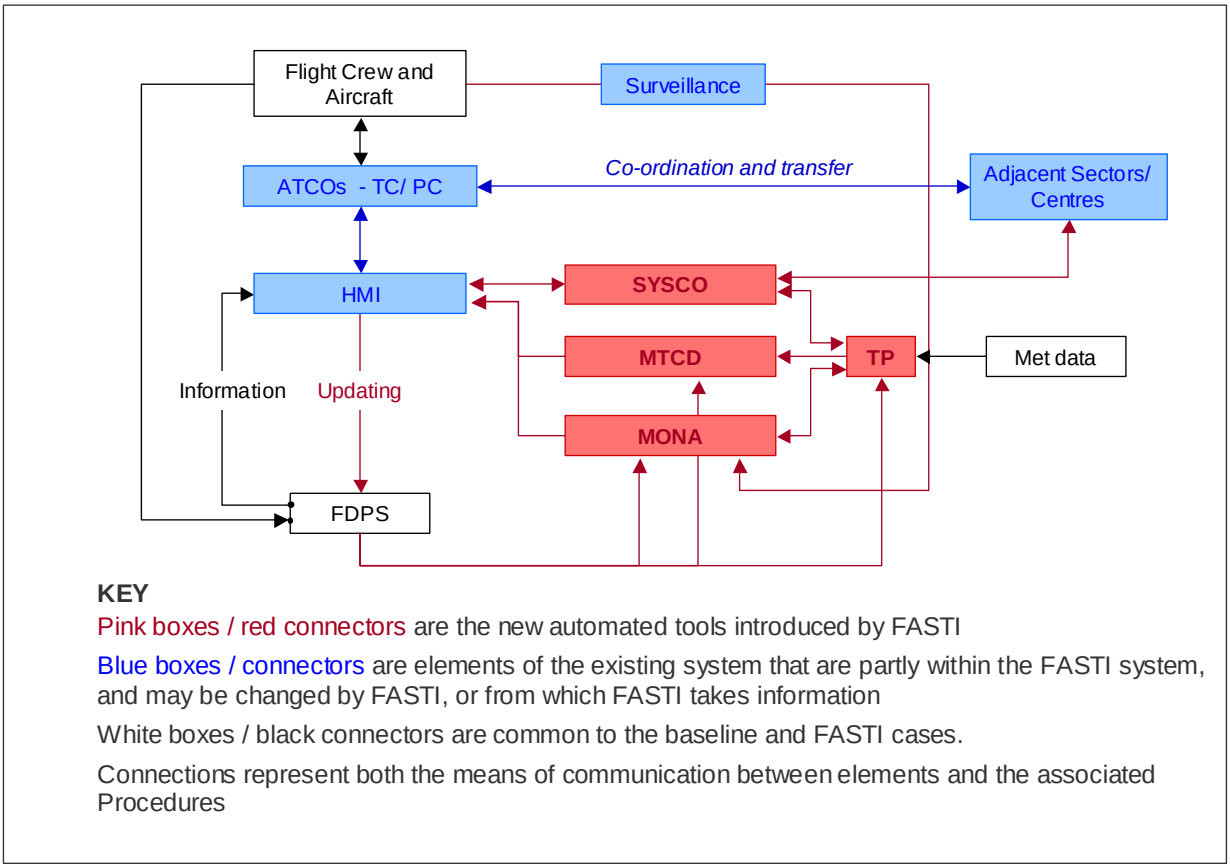

Figure 4 – Logical Model for FASTI

FASTI introduces new automated tools that support monitoring and co-ordination. Some functions currently performed by the controller are partly allocated to the automation, and some functions will be supported by the automation.

FASTI can be implemented at different levels of automation, i.e. with different degrees and scopes of delegation from human to automation. However, the proposed general principles for sharing of responsibility between controller and automation are that:

- the automation is responsible for detecting conflicts and non-conformances between flights operated within prescribed conditions;
- the automation is responsible for warning the controller when it is unable to detect a conflict or non-conformance (for example because the flight does not meet the prescribed conditions or because some information is missing);
- The controller is responsible for issuing clearances that ensure separation.

The new automated tools are as follows:

- **MTCD** detects conflicts in the medium term. This reduces dependence on vigilance of the PC. It will help not only in detecting problems but also in 'confirming' where no problems exist and hence saving unnecessary scanning time. MTCD also supports conflict resolution, by providing a 'what-if' probing function, and identifying aircraft constraining the resolution of a conflict or occupying a flight level requested by another aircraft. It also issues reminders when actions are due. MTCD is seen as principally a tool for the Planner role.
- **MONA** detects actual or anticipated deviations from the system trajectory, such as non-conformances against flight planned route or flight level or against clearances. MONA thus reduces dependence on controller vigilance. It will help not only in detecting problems but also in 'confirming' where no problems exist and hence saving unnecessary scanning time. MONA also provides reminders to the controller when actions are due (e.g. control clearance (start of manoeuvre), transfer of communications to the next sector/centre, manual coordination required, route clearance after an open vector instruction). MONA triggers the trajectory recalculation process when required, i.e. following a controller input that changes the planned trajectory or a change in aircraft trajectory (following a clearance). The re-calculated trajectory updates the information provided to MTCD. It is not necessary that all these functions are implemented together: implementers may choose to deploy specific sets of warnings and reminders. Additional functions can also be derived from the use of TP (e.g. area infringements). MONA supports both PC and TC roles.
- **SYSCO** supports co-ordination between PCs in different sectors or centres, by facilitating screen-to-screen exchange of information rather than by voice. It thus reduces the workload associated with telephone co-ordination. It thus facilitates earlier resolution of conflicts, improves controller situational awareness and can enable new operational concepts such as MTCD planning. Coordination is performed automatically between sectors or centres on the basis of sector boundary conditions contained in the trajectory; the trajectory is also amended by sector boundary conditions received from external units. FASTI will provide procedures and guidelines for uniform use of this automated coordination, resulting in more silent coordination. Within the remit of FASTI, there are three areas in which CORT can be enhanced: the OLDI enhancements, SYSCO Level 1 transfer of communication (handover) functions and SYSCO Level 2. Further details of these enhancements can be found in [Ref 10]

MONA and MTCD rely on accurate flight plan data from the **FDPS**. Because of this, it is important for the Controller to keep the FDPS updated whenever he/ she changes an aircraft's trajectory

The three main tools are supported by, and interact, with **TP**. TP has two main 'engines': intent generation, containing models of the operational context and user preferences, and trajectory computation, which contains

aircraft performance and environment models. For FASTI, TP would be used in relation to two classes of trajectory:

- The planned trajectory: a medium-term view initially built in accordance with the flight intent, as described by the Flight Plan, and constrained by ATC procedures. Once the flight is active, the trajectory can be modified by ATC instructions, and by the integration of flight progress. The planned trajectory is the basis upon which (*inter alia*) flight data are distributed to the sectors traversed, coordination is performed between sectors, sector planning and MTCD are performed, and relative to which deviations are monitored by MONA.
- The tactical trajectory provides a short-term view taking account of the latest tactical clearances given to a flight, but without making assumptions on future clearances to be given. The tactical trajectory is used in the detection of conflicts involving aircraft on open clearances – i.e. where a further clearance is required in order for the aircraft to return to its own navigation of the planned intent.

2.4 Overall picture

The FASTI tools work *synergistically* together. For example, SYSCO supports not just co-ordination and transfer *per se*, but also helps with strategic resolution of conflicts, that may have been detected by MTCD, by allowing adjacent sector controllers to agree more easily to a change of entry or exit levels.

By providing this automated support, FASTI should enable controllers to work at a higher level, resulting in a shift from sector-focussed, tactical and reactive operational behaviour to trajectory oriented, strategically-planned, conflict-free behaviour. This offers the benefits of a more stable traffic flow and more effective and efficient control.

3. OVERALL SAFETY ARGUMENT

The main arguments supporting the claim that FASTI is acceptably safe in operation are presented in graphical form (Goal Structuring Notation, as described in the SCDM) in Figure 5.

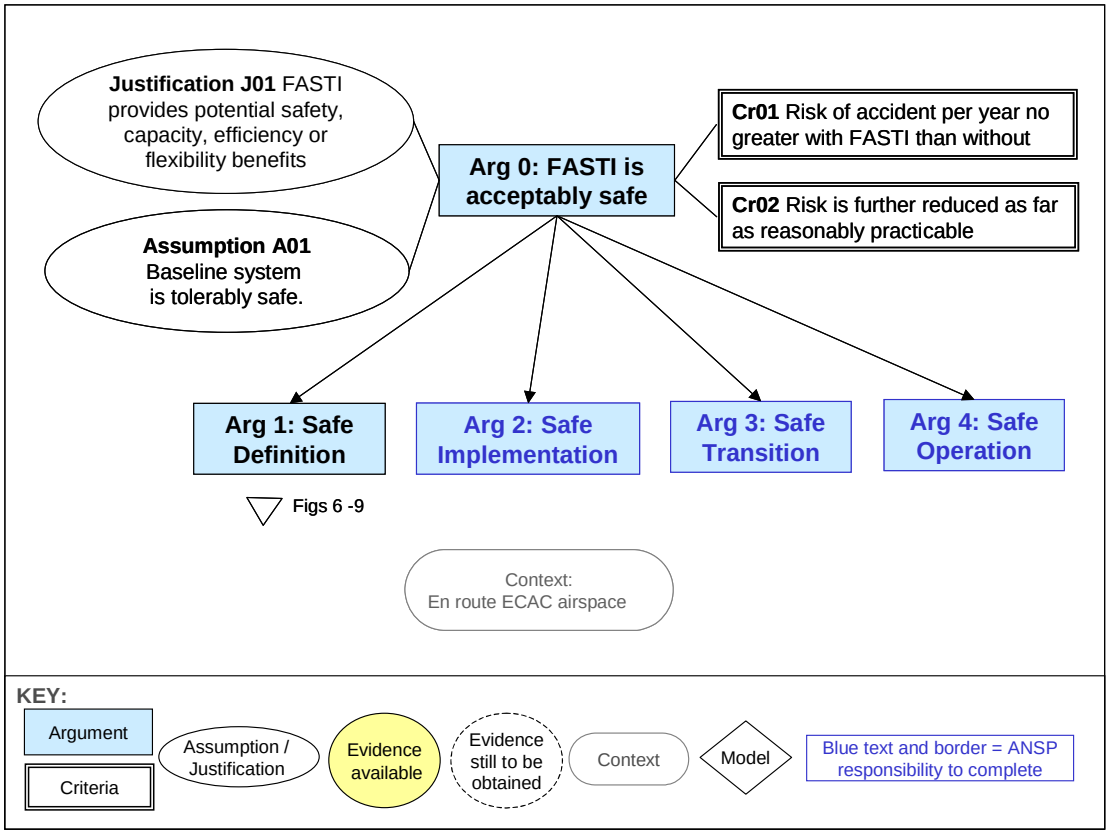

Figure 5 The Overall Safety Argument

3.1 The Claim

The top-level claim (Arg 0) is that FASTI will be acceptably safe in operation.

3.2 Criteria – how safe is acceptably safe?

Since safety cannot be absolute, it is necessary to define what is meant by 'acceptably safe'. Two criteria have been adopted, in line with generic EUROCONTROL safety policies [Refs: 13, 14], as follows:

Cr01: the probability per year[1], of an accident[2] in the affected airspace following the full deployment of FASTI shall be no greater than that for the baseline[3] system as defined in Section 2.

[1] Risk is measured per year, rather than per movement or per flight hour, in order to reflect the policy that accidents per year should not increase, despite growth in traffic [Ref.12]

Cr02: the probability of an accident following the deployment of FASTI shall be further reduced as far as reasonably practicable.

3.3 Justification

For EUROCONTROL, FASTI is one of several programmes designed to help co-ordinate and facilitate the harmonised implementation of measures for safe management of air traffic growth across Europe. FASTI is intended to provide potential benefits in terms of safety, capacity and efficiency, and also to act as an enabler for further advances in automation. The FASTI programme recognises that, while the greatest benefits will come from pan-European implementation, different ANSPs have different starting points and priorities, and such changes cannot be introduced all at once. Hence it is aimed at individual ANSPs and centres, encouraging the introduction of the new tools by each, but in a harmonised way.

Individual ANSPs will have varying justifications for implementing FASTI. Some ANSPs may wish to take all the benefits of FASTI in terms of safety improvement, while others may wish to trade some or all of this benefit for gains in capacity or efficiency. This will be a matter for individual ANSPs and their national regulators to decide, with due regard to wider EC and EUROCONTROL safety aims. They will also need to show how any increases in capacity or efficiency are justified in relation to transport and environmental policies (see Argument 1.1.3)

By defining the criteria in Section 3.2, EUROCONTROL aims to ensure that the overall effect on safety will always be positive. Cr01 ensures a net safety benefit from introducing FASTI, wherever an ANSP decides to set the balance between safety, capacity and efficiency. Cr02 requires ANSPs to deliver safety improvements over and above the minimum requirement expressed in Cr01, 'as far as reasonably practicable'. States and ANSPs will differ in how they interpret this term, and their different contexts will affect what it means in practice, but all are required to consider carefully how risk can be further reduced.

3.4 Context

A system is only safe in a particular environment. It is therefore necessary to define the environment for which the system is designed. For ATM systems the environment is usually referred to as the operational context.

The operational context for which FASTI is designed is en-route airspace in the ECAC area; although this may border on terminal airspace,

[2] A Severity Category 1 event, as defined in ESARR 4 [Ref.4].

[3] The baseline system is that as defined in Section 2 and Appendix C. Although ANSPs will in practice start from different actual baselines, it is important that safety should be tested against a consistent baseline. Otherwise, an ANSP could claim a safety benefit for the enablers necessary to bring the system up to the baseline, and ascribe that benefit to their 'FASTI project'. This could distract from the effort necessary to ensure that FASTI itself (relative to the baseline) is safely implemented.

uncontrolled airspace, non-ECAC airspace etc. The interfaces with these areas are taken into account in the Safety Argument.

3.5 High-level assumptions

It is assumed (**A01**) that the typical European ATM system into which FASTI will be introduced (i.e. the baseline as defined in Section 2, in its current operational context) is, currently, acceptably safe. This establishes the safety baseline for FASTI, which seeks to improve on, or at least not degrade, the current level of safety (**Cr01**).

This remains an Assumption, because, although the risk associated with ATM has, *de facto,* been 'tolerated' by society, it has not been demonstrated the risks are acceptable in any more formal sense. Existing ATM systems as a whole have not been subjected to comprehensive, rigorous safety assessment or consideration of tolerability, either at ECAC-wide level or within most individual ANSPs.

3.6 Strategy – the argument structure

EUROCONTROL is developing a generic Safety Argument that can be applied to a wide variety of ATM systems [Ref 15]. The FASTI Safety Argument has been based closely on this generic structure.

The top-level Claim is supported by four main arguments (**Arg 1** to **Arg 4**), reflecting the lifecycle stages (as described in Section 1.4), as follows:

> **Arg 1:** Definition: the FASTI concept and high-level design have the potential to be acceptably safe – i.e. they are capable of satisfying the safety criteria, assuming that a suitable detailed design could be produced.
>
> **Arg 2:** Implementation: the detailed design is in accordance with the definition. Also, procurement, construction, integration and commissioning are performed safely.
>
> **Arg 3:** Transition from the old to the new system is performed safely.
>
> **Arg 4:** Operation – the operational use of the system, including its maintenance and updating, continue to be acceptably safe.

Using an argument structure that has already been applied to several ATM systems, and that should become increasingly familiar to stakeholders, makes good use of lessons learned and will facilitate development, review and auditing of the full Safety Cases, both internally by ANSPs and by regulators.

More specifically for FASTI, a lifecycle-based structure also has the advantages that it clearly reflects the distinction between the roles of EUROCONTROL and the ANSPs, and that it covers the main safety issues in developing and implementing new systems without too much focus on the details of specific tools (which may change over time and between ANSPs).

Each main argument is broken down to lower levels of detail. Note that Arguments only need to be developed to a level at which Evidence is available, or could feasibly be provided, to substantiate the Argument.

Sections 4 to 7 following present each of the four main Arguments, together with:

- the Evidence substantiating the Argument;
- any **Safety Issues**, that EUROCONTROL will need to address in order to complete the PSC;
- **Safety Recommendations**: practical means by which the Safety Issues could be addressed;
- **Safety Requirements** on the system that each ANSP will need to ensure are satisfied. Safety Requirements (SRs) are practical design requirements on the functionality, performance, reliability or integrity of the operational system to ensure that the Arguments and Evidence offered 'in principle' in this PSC become true in practice. Safety Requirements are designated SR-nn-XX, where nn denotes the Logical Model element to which they refer and XX is a reference number.
- **Guidance** – outlining what ANPSs will need to do to complete the Safety Case, by identifying specific key areas in which they will need to review or develop the Arguments and Evidence. More detailed support for ANSPs is available in the Guidance Document [Ref.1]

4. SAFETY OF FASTI DEFINITION (ARG 1)

This Section presents the more detailed Arguments and Evidence for the safety of the Definition stage of FASTI. It is argued that the FASTI concept and high-level design are acceptably safe in principle – i.e. subject to subsequent safe implementation, transition and operation.

The overall strategy has been to break down Arg 1 into sub-arguments, about the concept, about the high-level design, and about external and internal failures and then to provide general backing evidence regarding the quality of the safety work, and the realism of the Safety Requirements. These sub-arguments closely follow those in the EUROCONTROL Generic Safety Argument [Ref.15], and are as follows:

- **Arg 1.1:** The concept is intrinsically safe
- **Arg 1.2:** The high-level design is complete
- **Arg 1.3:** The high-level design is correct and coherent
- **Arg 1.4:** The high-level design is robust against external failures, errors and abnormalities
- **Arg 1.5:** Risks from internal failures within the FASTI system are sufficiently reduced
- **Arg 1.6:** All Safety Requirements are realistic and demonstrable – i.e. capable of being achieved in practice by typical ANSPs and demonstrable as having been achieved
- **Arg 1.7:** The safety assessment has been suitable and sufficient.

Sections 4.1 to 4.7 following discuss each of these sub-Arguments, together with the related Evidence, any Safety Issues and Safety Recommendations for EUROCONTROL, and the Safety Requirements and outline Guidance for ANSPs.

4.1 Arg 1.1- Intrinsic Safety of the Concept

Aim and Strategy:

Arg 1.1 aims to show that the FASTI concept is intrinsically safe – i.e. that it has the potential to deliver its non-safety benefits whilst meeting the safety criteria – i.e. providing at least the same level of safety as the baseline case.

The argument has been broken down into lower-level arguments as described in more detail in the following text.

Arg 1.1.1 *The overall safety aims have been identified*

Evidence:

The key safety-related intentions behind FASTI, as described in Section 2, are to improve the strategic Conflict Avoidance barrier by supporting its associated functions, namely monitoring for conflicts and non-conformances and taking actions to resolve them, and co-ordination and transfer between sectors.

FASTI is intended to be as broad as possible in scope. For example the Operational Concept [Ref 5] notes that MTCD has to be designed to work for many different types of conflict: crossing, converging, opposite direction, catch-up and climb/descent conflicts as well as airspace conflicts and combinations of any of these conflict types.

Arg 1.1.2 *A Functional Model has been developed that completely and correctly interprets the Concept of Operations*

Evidence:

A general Functional Model of ATM has been developed and is described in Section 2.3. This model sets out how ATM will operate with FASTI implemented. (In fact, the model was been developed for ATM in general – at the abstract level, FASTI does not change the functions of ATM- see Arg 1.1.3 following).

Arg 1.1.3 *The differences from existing operations have been fully described and understood*

Evidence:

The functionality of ATM is not changed at the abstract level, but FASTI will change the demands placed on different elements of the Functional Model, as follows:

- the performance of SCD, SCR, FPM and CORT will be improved;
- greater demands will be placed on SFP, in that FASTI relies on flight plan data being accurate and up-to-date; and
- it is expected that there will be fewer demands on Flight Interaction, since the more pro-active approach to control should require fewer tactical interventions. This more pro-active control may also facilitate FM and CM.

Differences in terms of the allocation of functions between system elements are described in Arg 1.2.1.

Guidance Because the functional scope of the automated tools is flexible (MONA for example could be implemented to detect area infringements as well as non-conformances in route and level) ANSPs will need to review and define these differences in greater detail.

Arg 1.1.4 *The impact of the concept on the external operational environment and airspace has been assessed and shown to satisfy the safety criteria*

Aim and Strategy:

This Argument relates to the interfaces between FASTI and non-FASTI airspace, at the functional level. More detailed consideration is given to the interfaces with specific elements of the ATM system (as shown in the Logical Model) in Arg 1.2.

Evidence:

Because the FASTI concept is intended for en-route airspace in the ECAC area, the key interfaces to consider in this argument are those with the neighbouring, non-FASTI airspace. This may be terminal airspace, uncontrolled airspace, and/or non-ECAC airspace.

FASTI may enable certain changes and reductions in procedural constraints within FASTI airspace, in the interests of flexibility. These may have implications for adjacent airspace.

SR-FAS-01 Co-ordination and Transfer procedures and LOAs between the FASTI airspace and non-FASTI airspace shall be adapted where necessary to accommodate changed procedures within the FASTI airspace

Controllers in FASTI centres may need to communicate with their counterparts in non-FASTI centres.

SR-FAS-02 Controllers in FASTI airspace shall retain an understanding of telephone-based co-ordination. In particular they shall retain the voice communication skills necessary to communicate with their counterparts in non SYSCO-equipped airspace.

The above SRs are likely to be incomplete, as the Operational Concept does not yet consider impacts on neighbouring non-FASTI airspace.

Safety Issue: The FASTI Operational Concept needs to be developed to identify and address, comprehensively, issues relating to interfaces with and impacts on neighbouring non-FASTI airspace

Arg 1.1.5 *The FASTI concept has the potential to satisfy the safety criteria for the overall ATM system*

Aim and Strategy:

This Argument is divided into two branches, considering each of the safety criteria **Cr01** and **Cr02** defined in Section 3.2.

These arguments show that the FASTI concept will satisfy the criteria, subject to appropriate design, implementation, transition and operation.

Arg 1.1.5.1 *The FASTI concept will satisfy criterion Cr01*

The aim of this Argument is to show that FASTI can improve, or at least maintain, the level of safety provided by the existing (baseline) ATM system.

Evidence:

In terms of the Barrier Model, the crucial difference from the current system is that FASTI enables the *Conflict Avoidance* barrier to be strengthened. It improves the planning role in detecting and thereby removing conflicts, and so allows proportionally fewer conflicts through to the *Tactical Deconfliction* barrier, placing less demand on it.

FASTI is not in itself designed to change the performance of other barriers. Cases in which other barriers are deliberately weakened, or a greater input (i.e. traffic) allowed in order to gain capacity, efficiency or flexibility benefits are considered in Arg 1.1.5.2. Thus, if all other barriers remain as effective, and if the traffic throughput remains the same, there would be fewer *Separation Infringements* and consequently a lower risk of accident.

In summary therefore the Evidence is that, by making the Planner function in ATM more effective in detecting, and thereby removing, conflicts before they progress to the Tactical stage, and because it does not in itself weaken other barriers, FASTI has the potential to improve safety within FASTI airspace, and hence to satisfy **Cr01**.

Arg 1.1.5.2 *The FASTI concept will satisfy criterion Cr02*

The aim of this Argument is to show that FASTI enables risk to be made AFARP.

Evidence:

FASTI's potential to improve safety may to some extent be traded off for other types of benefit: capacity, efficiency/ flexibility or combinations thereof. In terms of the Barrier Model, this involves deliberately not taking all the potential advantages related to Conflict Avoidance as safety benefit, weakening other barriers or allowing an increase in the input to the system – i.e. increased traffic.

FASTI could enable a capacity benefit: i.e. more traffic being handled for the same level of safety. In Barrier Model terms, a higher traffic level would lead to a greater number of potential conflicts at the input to the model, but this would be compensated for by the increase in the conflict-reduction capability of the Collision Avoidance barrier, resulting in the same conflict-resolution demand on the ATC Deconfliction barrier and hence in the same number of Separation Infringements and accidents.

FASTI does not in itself weaken other barriers, but could enable improved efficiency or flexibility of the ATM service by, for example, allowing more direct routeing of aircraft and removing some constraints on ATC practices (further examples are given in Section 2.1). These changes might weaken the Airspace Design or Procedural Deconfliction barriers, but again this would be compensated for by the strengthening of the Conflict Avoidance barrier.

From the above it can be seen that FASTI concept allows flexibility to obtain a pure safety benefit, or to trade this for other types of benefit: capacity, efficiency/ flexibility or combinations thereof. It will be for individual ANSPs to make these AFARP decisions, in the light of their specific operational context, business drivers and regulatory regimes.

Guidance: Each ANSP must justify how they have decided on a balance between safety benefits and capacity/ efficiency/ flexibility benefits that is appropriate to their own operational context and needs. Due regard must be given to the national and internal safety regulation regime and to wider EC and EUROCONTROL safety aims. ANSPs will also need to show

how any increases in capacity are justified in relation to transport and environmental policies.

Arg 1.1.6 *The key functionality and performance parameters that affect safety have been defined and are compatible with the Safety Criteria*

Evidence:

The functionality and performance parameters of FASTI that are critical to its success in safety terms are as follows:

a) the increase in the proportion of conflicts that are detected and resolved at the Planning stage;

b) the increase in the proportion of non-conformances that are detected and resolved at the Planning stage; and

c) the effectiveness with which the Flight Plans are kept up to date.

Parameters (a) and (b) relate to criterion Cr01. If en-route ATM accident rates are not to increase despite growth in traffic, innovative measures will be needed to improve conflict detection and resolution. FASTI is intended to enable more conflicts and non-conformances (which potentially lead to conflicts) to be detected and removed at the planning stage, as this has the potential to be both more efficient and safer than leaving them to the tactical stage. It is therefore critical to the success of FASTI that the proportions detected and resolved during Planning should increase.

Parameter (c) is critical because FASTI relies on accurate and up-to-date FP information within and between sectors.

Guidance: ANSPs should define thresholds of acceptability for each of the key functionality and performance parameters, and refine their definitions if required, in order to reflect the specific level of safety (and other) benefits that they require from FASTI.

Safety Issue: EUROCONTROL should consider whether it may be possible to define example thresholds of acceptability for each of the key functionality and performance parameters for a typical implementation (e.g. MUAC)

Conclusion to Arg 1.1

With the exception of the following Safety Issues, there is sufficient evidence from the lower level arguments to provide confidence that the FASTI concept is intrinsically safe.

The outstanding Safety Issues are:

- The FASTI Operational Concept needs to be developed to identify and address, comprehensively, issues relating to interfaces with neighbouring non-FASTI airspace; and
- EUROCONTROL should consider whether it may be possible to define example thresholds of acceptability for each of the key functionality and performance parameters in a typical implementation.

4.2 Arg 1.2 - The FASTI high-level design is complete

Aim and Strategy

Arg 1.2 aims to show that the high-level design of FASTI, so far as it can be defined by EUROCONTROL at this stage, contains everything necessary to embody the concept and, more specifically, that it has the potential to deliver the core functionality as defined in Arg 1.1.

Arg 1.2 has been broken down into sub-arguments as described further in the following text.

Arg 1.2.1 *The high-level design and its rationale are fully documented*

Aim and Strategy:

This Argument aims to show that a Logical Model has been developed that completely and correctly interprets the concept and the functional model in terms of an architecture of people, procedural and equipment elements.

The main features of the high-level design are shown in the Logical Model (Figure 4) and are described in Section 2.3. In summary, FASTI introduces three new tools (MTCD, MONA and SYSCO) to automate and/or support, respectively, conflict detection, conformance monitoring and CORT. These tools depend on and interact with information from the FDPS, TP, and surveillance systems.

This argument is further divided into fourth-level arguments as described below.

Arg 1.2.1.1 *The boundaries of the system are clearly defined*

Evidence

Because ATM is a highly interdependent system, into which FASTI will be integrated, it is not possible to draw a simple physical boundary around the FASTI system, as one might for a simple stand-alone system, such as an anemometer. Rather the Logical Model shows the boundaries in terms of:

- the new tools: MTCD, MONA, SYSCO and TP;
- elements of the existing ATM system that interface with FASTI: and may therefore need to be changed to some extent: the HMI, surveillance, the FDPS and adjacent sectors/ centres; and
- elements that will not change: there is for example no direct impact on flight crew or aircraft.

Arg 1.2.1.2 *Differences from the baseline have been identified*

Evidence:

The key difference between the FASTI high-level design and the current (baseline) is that a proportion of the tasks of monitoring for conflicts and non-conformances are allocated to the automation rather than to the human. The automation also supports resolution of conflicts and non-conformances by providing reminders of actions that are due. The automation also supports CORT.

The rationale for automating these particular aspects of the system is that routine monitoring and co-ordination tasks currently account for a high proportion of controller workload (time and cognitive resources). By providing this automated support, FASTI should enable controllers to work at a higher level of planning and problem solving, resulting in a shift from sector-focussed, tactical and reactive behaviour to trajectory oriented, strategically-planned, conflict-free behaviour.

Arg 1.2.1.3 *The Logical Model is complete*

The Logical Model has been reviewed against the Operational Concept [Ref 5] for completeness.

Table 1 provides further evidence of completeness by showing two-way traceability between the Logical and Functional Models. It shows how FASTI will change the way that certain functions of ATM (as described in the Functional Model of Section 2.2) are performed.

Table 1: Link between Functional and Logical Models

Function (from Functional Model)	**Allocation of Function (from Logical Model)**	
	Baseline	**With FASTI**
Coordination and transfer	Controllers, using LOA and OLDI v3 + basic messages and by voice	Controllers, with SYSCO facilitating more screen-to-screen co-ordination and greater automation. FASTI will provide procedures and guidelines for effective, uniform use of this automation, resulting in more silent coordination.
Strategic conflict detection	Controller	Controller, with MTCD taking a proportion of the monitoring task by providing automated early detection of conflicts
Strategic conflict resolution	Controller	Controller, supported by MTCD providing what-if probing and reminders of related actions
Flight progress monitoring - conformance monitoring	Controller	Controller, with MONA taking a proportion of the monitoring task by providing automated early detection of non-conformances
Flight progress monitoring – strategic/ tactical resolution of non-conformances	Controller	Controller, supported by MONA providing reminders of actions due

Arg 1.2.1.4 *Specific changes in working practices and controller cognitive activities have been identified*

Evidence:

More specific changes in working practices and controller cognitive activities that will result from implementation of FASTI have been identified in the CTA [Ref.16]. These changes and their potential effects on safety (either positive or negative) are shown in Table 2.

Table 2 Potential safety effects of changes in working practices and cognitive activity

Effect on working practices and cognitive activity	**Areas of potential safety impact**
Change in proportions of time and cognitive effort spent on different tasks	Error rates – up or down? Possible mismatch between trained and required skills and priorities
Changes in allocation of tasks and workload between PC and TC	Error rates – up or down? Possible mismatch between trained and required skills and priorities (Secondary) Workload changes – up or down?
Changes in nature and extent of communications between PC and TC	Error rates – up or down? Possible mismatch between trained and required skills and priorities Job satisfaction
Use of MTCD displays to build and update mental picture and situation awareness (SA). Rather than having a picture of current and future individual aircraft positions, the SA of controllers may be more in terms of sets of potentially conflicting aircraft	Quality of SA (improved?)
Controller use of presentation of conflicts on MTCD to retrieve the plan of action.	Improved(?) retrieval

The above changes have been identified as possibilities using a structured analytical process. They are not necessarily a complete set of potential changes, neither is the extent to which they might occur in practice known. The exact nature and direction of these changes cannot be foreseen in detail, as it will depend on a number of factors that are specific to the detailed design and implementation of the system**.**

Safety Issue The nature and extent of changes in working practices and cognitive activities resulting from implementation of FASTI need to be identified more robustly, and their effects on safety assessed. Where necessary, further work may be needed to mitigate any adverse effects and maximise beneficial ones.

Safety Recommendation: Changes in working practices and cognitive activities resulting from FASTI could be investigated by means of observations and structured debriefs during simulation, as well as by elicitation of findings from 'Pioneer' ANSPs who have already implemented FASTI-like systems. Any adverse effects will need to be mitigated and beneficial effects maximised by, for example, adjustments to the procedures or training.

Arg 1.2.1.5 *How FASTI is to be used - the relationship between human and automation - has been fully described*

Aim and Strategy:

At this high-level design level of the argument it is important to look further at how the system will be used by the controller - in particular at the relationship between human and automation.

Evidence:

FASTI introduces new automated tools that support monitoring and co-ordination. Some functions currently performed by the controller are partly allocated to the automation, and some functions will be supported by the automation. The general principles for sharing of responsibility between controller and automation are that:

- the automation is responsible for detecting conflicts and non-conformances between flights operated within prescribed conditions;
- the automation is responsible for warning the controller when it is unable to detect a conflict or non-conformance (for example because the flight does not meet the prescribed conditions or because some information is missing); and
- the controller is responsible for issuing clearances that ensure separation.

FASTI can be implemented at different levels of automation, i.e. with different degrees of delegation from human to the new automated tools. For example, notification of a conflict to the TC may be at the discretion of the PC or automated, once the time or distance to loss of separation falls below a certain user-specified threshold.

Decisions about the level of automation are essentially for ANSPs to define and justify in the light of their specific needs and context.

Guidance: The key considerations for ANSPs deciding how much automated support is needed are the current demands on controller workload as compared to the demands likely to be imposed by future traffic levels. Once the level of automation has been decided, safe use of the tools – in particular the task distributions between controllers and automation - will be ensured by defining prescribed working methods and procedures, and by designing appropriate affordances[4] for the tools and interaction objects on the HMI.

[4] Affordances [Ref 15] are the perceived or actual properties of things that determine, or provide users with clues to, how they can be used. For example, a

Arg 1.2.2 *The high-level design includes everything necessary to achieve a safe implementation of the concept*

Evidence:

The Logical Model shows the various ATM system elements necessary to implement the concept. Table 3 lists Safety Requirements related to each element of the FASTI system.

The Table includes Requirements on procedures related to each FASTI tool, as well as the hardware/ software elements. It has been derived by collating needs referred to in the Operational Concept, OSEDs, Logical Mode, the FASTI Baseline Description [Ref.18] and other descriptive material.

Some of these references contain additional, more detailed Requirements, some of which may be subject to change. This table generalises them to a level more appropriate to a generic PSC.

Table 3 Safety Requirements on each system element

SR no	Safety Requirement or Assumption
FASTI – general	
SR-FAS-03	High reliability and integrity[5] of all automated functions, including: – the detection of conflicts (MTCD) and non-conformances (MONA), – calculation of 'what-if' trajectories and checking them for other conflicts, – trajectory updating – algorithms for reminders – algorithms for transfers. – data transfer between elements and display on HMI.
SR-FAS-04	Support controller cognitive activity: allowing flexibility to adapt strategy to workload and to manage interruptions
SR-FAS-05	Facilitate the construction and refreshment of the controller's mental picture of the traffic situation
SR-FAS-06	Support the controller in monitoring potential problems which, due to uncertainty, will require re-assessment at a later time

door handle offers itself to be turned or pulled, whereas a flat door plate invites pushing.

5 Reliability and integrity are essential to the success of FASTI - the safety benefits and other benefits will not be obtained unless the system is dependable. In particular, the automated tools must be at least as good as the unaided controller or there will be no benefit. Also, without dependable behaviour, controllers will not trust and use the automation. Reliability and integrity are also important in preventing internal failures that can lead to hazards; this aspect – in which reliability and integrity are considered somewhat differently - is covered in Arg 1.5.

SR no	Safety Requirement or Assumption
SR-FAS-07	Facilitate cooperation between PC and TC, e.g. through sharing of appropriate information
SR-FAS-08	Procedures shall define working methods, procedures, roles and responsibilities to enable the controllers to work effectively and efficiently with the tools.
SR-FAS-09	Have an appropriate level of 'intelligence' in the algorithms for alerts etc. The balance needs to be optimised between 'crude but effective' solutions and solutions that which are more sophisticated, but less easy to implement.
MTCD	
SR-MTCD-01	Identify potential conflicts, with sufficient warning time (taking account of delivery, read back and aircraft manoeuvre times) but minimising nuisance alerts.
SR-MTCD-02	Identify all conflicts of relevance to the controller. This could include, for example: • entry, exit and in-sector conflicts, but not entry conflicts that are the responsibility of the preceding sector. • conflicts related to both open and closed clearances (i.e. whether or not a further clearance is required to return the aircraft to its plan) conflicts between aircraft where neither, one or both are deviating from their clearances • flights whose separation on entry or exit is not in accordance with the relevant Letter of Agreement (LOA)
SR-MTCD-03	Facilitate efficient conflict management e.g. by highlighting groups of conflicts that could be resolved by taking action of a single aircraft
SR-MTCD-04	Assist the controller in verifying alternative routeings or levels (e.g. by providing a 'what-if' probe, indication of available alternative levels, indication of constraints)
SR-MTCD-05	As appropriate, transfer conflicts requiring tactical intervention automatically from PC to TC for resolution, and/ or allow the PC to do so.
SR-MTCD-06	Amend conflict indications according to the clearances issued (and entered into the system) by the controller
SR-MTCD-07	Have thresholds and procedures harmonised with those of STCA and ACAS and other conflict management tools and safety nets.
SR-MTCD-08	Issue reminders to the controller when actions are due
SR-MTCD-09	Support prioritisation when multiple conflicts occur
MONA	
SR-MONA-01	Identify when aircraft actual or predicted aircraft positions and trajectories deviate from: - their clearance - the sector flight plan - the airspace definition and restrictions - agreed co-ordinated transfer conditions with sufficient warning time (taking account of delivery, read back and aircraft manoeuvre times) but minimising nuisance alerts.

SR no	Safety Requirement or Assumption
SR-MONA-03	Update the trajectory of each aircraft following a manual update or an automatic change through electronic co-ordination (SYSCO) or CPDLC clearance
SR-MONA-04	Distinguish between different aircraft states (e.g. ACT-in, assumed, etc)
SR-MONA-05	Issue reminders to the controller when actions are due
SR-MONA-06	Facilitate controller interaction with the aircraft predicted trajectory (trajectory editor function)
SR-MONA-07	Facilitate trajectory updates (TPU function)
SR-MONA-08	Support prioritisation when multiple non-conformances occur
SYSCO	
SR-SYS-01	Enable screen-to-screen co-ordination and transfer dialogues between controllers in adjacent sectors
SR-SYS-02	Support prioritisation when multiple messages are pending
SR-SYS-03	Allow the PC to counter-propose entry conditions with preceding sector/ centre
SR-SYS-04	Allow the PC to amend exit conditions, revising any already existing co-ordination with the succeeding sector/ centre
TP	
SR-TP-01	Calculate predicted aircraft trajectories of the aircraft up to x minutes ahead
SR-TP-02	Pass predicted trajectory information to FASTI tools
SR-TP-03	To ensure that TP, and hence MTCD and MONA, are available for aircraft as they enter the FASTI airspace, there must be an adequate overlap of the necessary surveillance and prediction functions into the upstream sector
Controller	
SR-CON-01	Manage actions related to the analysis and resolution of problems (conflicts or non-conformances) until they are of no further interest
SR-CON-02	Take account of the displayed MTCD and MONA warnings and reminders in the controlling process
SR-CON-03	Where appropriate, respond to / acknowledge alerts and messages from MTCD, MONA and SYSCO
SR-CON-04	Update flight plans (ground system trajectories) whenever needed (e.g. following a clearance/instruction)
SR-CON-05	Remove reminders after a performed action
HMI (generic requirements – requirements related to the display of specific tool-related information are	
SR-HMI-01	Display FASTI-specific information, principally: - conflict warnings - non-conformance warnings - action reminders - SYSCO dialogues
SR-HMI-02	Facilitate controller interaction with the tools – eg click on conflict warning to display more detail or enter data into SYSCO dialogues

SR no	Safety Requirement or Assumption
SR-HMI-03	Display information and facilitate interaction in accordance with current EUROCONTROL best practice guidance on interactivity, affordances, alert prioritisation, style, symbology and fonts, while at the same time being compatible with existing HMI.
SR-HMI-04	Integrate the new FASTI-specific display / interactivity elements , such as MONA/ MTCD alerts and SYSCO dialogues, with the existing ones effectively and without excessive clutter or potential for confusion (Consider for example providing controllers with the ability to reduce display clutter by setting appropriate conflict alert thresholds for the particular conditions)
SR-HMI-05	Facilitate controller updating of ground system trajectories whenever needed
SR-HMI-06	Display the time to conflict and predicted minimum separation that will be obtained between controller-selected aircraft
SR-HMI-07	Display appropriate views of the conflict / non-conformance geometries e.g. horizontal and vertical views
SR-HMI-08	Indicate when a conflict or non-conformance is amended or no longer exists
SR-HMI-09	Where appropriate, permit the controller to remove from display alerts that he/ she considers unnecessary

Guidance: ANSPs may, in the light of their context, needs and emerging design and implementation plans, and with sufficient reason documented in their Safety Cases, decide not to implement all of the above SRs, to amend them or to introduce additional ones.

Arg 1.2.3 *Dependencies on and assumptions about the external systems with which FASTI interfaces have been identified*

Evidence:

Interfaces with external systems are shown in the Logical Model. The dependencies and related Assumptions are as follows:

FDPS. FASTI tools are – as recognised in Arg 1.1.6 - critically dependent on up-to-date information from the FDPS. Without this, accurate detection of conflicts and non-conformances is impossible. Hence, as well as the requirement for controllers to keep the FDPS up-to-date (SR-CON-4), there is an Assumption **(A02)** that the FDPS itself is of sufficiently high functionality, performance, reliability and integrity to provide the information needed by FASTI.

Surveillance systems. FASTI relies on surveillance to provide information on current aircraft positions and vectors, using these data in TP and hence in the detection of conflicts and non-conformances. Therefore, there is an Assumption **(A03)** that the surveillance system is of sufficiently high functionality, performance, reliability and integrity.

Meteorological data systems. FASTI uses meteorological data in the environment model of TP. Hence there is an Assumption **(A04)** that the meteorological datasystem is of sufficiently high functionality, performance, reliability and integrity.

Adjacent sectors/ centres. FASTI interfaces with adjacent sectors/ centres both directly, in relation to SYSCO co-ordination, and in terms of the need to consider how FASTI-equipped centres/ sectors will need to interface with those that are not FASTI-equipped. It is therefore an Assumption **(A05)** that suitable co-ordination and transfer procedures and LOAs, revising existing ones where necessary, can be agreed with non-FASTI centres.

Conclusion to Arg 1.2

The evidence for the lower level arguments provides confidence that the high-level FASTI design is largely complete and that Safety Requirements have been defined to embody the concept and deliver its core functionality safely.

The main exception is that the nature and extent of changes in working practices and cognitive activities resulting from implementation of FASTI need to be identified more robustly, and their effects on safety assessed. This will principally be achieved through simulation. Depending on the findings, further work may be needed to mitigate any adverse effects and maximise beneficial ones.

4.3 Arg 1.3 - The FASTI high-level design is coherent and correct

Aim and Strategy:

The argument is that the FASTI high-level design is internally coherent - all data are from consistent and up-to-date sources, there is consistent use of data throughout the system and consistent functionality. It is also argued that the high-level design is correct – it carries out the functions effectively and efficiently. So this is an argument about performance as well as functionality.

Arg 1.3 has been broken down into sub-arguments as described in the following text.

Arg 1.3.1 *All reasonably foreseeable normal operational conditions and range of inputs from adjacent systems have been identified*

FASTI needs to operate safely over the full range of conditions that may be encountered in European en-route airspace.

Evidence:

Stakeholder involvement, through the OFG and the hazard identification work to date has helped to ensure that a wide range of operational conditions have been taken into account in the development of FASTI. This has been augmented on the basis of experience and brainstorming exercises conducted for similar projects. The parameters that define operational conditions can be summarised as below:

- traffic levels;
- complexity of traffic pattern (e.g. proportion of climbing / descending traffic, crossing traffic);

- airspace (class, size of sector/ centre);
- presence of Temporary Segregated Areas (TSAs) and procedures for their activation/ deactivation;
- traffic patterns (e.g. how to allow for holding);
- controller shift handover procedures;
- operational context of adjacent centres (including whether or not FASTI-equipped);
- aircraft performance (speeds, climb/ descent rates, turn rates);
- aircraft equipment fit (navigation systems ..);
- air operator procedures (for both civil and military operators) e.g. response times; and
- weather conditions:
  - wind (affecting ground speeds),
  - thunderstorms, icing, turbulence and other adverse conditions that may result in individual aircraft requesting level/ heading changes at short notice, or constraints on airspace availability.

Safety Issue: suitable ranges of possible values for these parameters will need to be decided on for simulation. The aim should be to test FASTI under a range of conditions that typify the range encountered in implementing centres, although it would of course be impracticable to test every possible combination that might affect it.

Guidance: ANSPs will need to identify, by brainstorming and analysis of data, the types and ranges of parameters that may affect FASTI under their own operational conditions.

Arg 1.3.2 *The high-level design is internally coherent*

Aim and Strategy:

The FASTI system and its component tools need to be provided with consistent and up to date data, both within and between sectors, under all the normal operational conditions identified in Arg 1.3.1, and to use these data in consistent ways. It must be ensured that there are no conflicting indications, and that assumptions and approximations used are consistent.

Evidence:

The information flows at the highest level are shown in the Logical Model.

The requirement on controllers to update the system whenever an instruction is issued or other changes are made, and the corresponding requirement for the HMI to facilitate such updating, have already been noted as SR-CON-04 and SR-HMI-05 under Arg 1.2.2.

The evidence for this argument has not been developed in greater detail in the present PSC as the operational concept and high-level design documents do not contain sufficient detail of the information flows between system elements; the elements of the Logical Model are largely described as stand-alone elements. It is debatable how far the EUROCONTROL concept and high-level design should develop such information and how much should be left for implementing ANSPs. However, it is suggested that, as a minimum, EUROCONTROL should conduct an initial walk-through analysis of the high-level data flows.

Safety Issue EUROCONTROL should analyse the high-level data flows between system elements and hence identify any additional Safety Requirements for internal coherence that may be required. Having done this, EUROCONTROL should decide how much further to go in defining the information flows between system elements in greater detail.

Safety Recommendation The analysis of design coherence should be performed in structured brainstorming/ analysis systems with design and operational experts, conducting a walk-through of a number of scenarios and 'what-if situations' (e.g. 'what if the PC passes this conflict to the TC'. This walk-through should be done before and in preparation for the simulations, as it will help ensure that simulations cover all the important aspects that can be simulated, as well as revealing issues that cannot be simulated.

However far EUROCONTROL decides to go in defining information flows between system elements, there will always be detailed matters that depend on specific technical implementations – i.e. on the hardware and software at individual centres, and how the FASTI tools are integrated with existing systems. These will need to be considered by the ANSPs.

Guidance ANSPs should develop more detailed Safety Requirements for data flows and consistency as part of their detailed design

Arg 1.3.3 *The high-level design functions correctly under all reasonably foreseeable normal operational conditions*

This argument is concerned with showing that the high-level design can function correctly under all reasonably foreseeable normal operational conditions, as identified in Arg 1.3.1. FASTI must work safely with the associated ranges of inputs from adjacent systems and the environment, both in steady states and dynamically (i.e. as conditions change).

Evidence:

We consider theoretical and practical evidence, some of which is already available, and the simulation evidence that will need to be gathered.

Theoretical evidence

For some parameters, it is possible to undertake theoretical analysis of the correct functioning of the design under specific parameter value combinations. For example it is possible to show, by collision risk calculations, that an MTCD tool can detect conflicts within a given time for a range of aircraft speeds and conflict geometries [Refs]? Theoretical

work has also been done by EUROCONTROL and others on TP performance

Safety Issue – A walk-through analysis of various scenarios should be performed in order to consider correct functioning of each element in the Logical Model.

Safety Recommendation This could effectively be combined with the walk-through of design coherence as described in the Safety issue for Arg 1.3.2.

Practical evidence

Some practical evidence that FASTI can operate safely across the range of normal conditions is available from the experience of ANSPs who have already developed and implemented, to varying degrees, similar tools in France, Germany and the UK [18]. Evidence is also available from EUROCONTROL's trials of MTCD at Malmo and Rome [Refs 19,20].

The references quoted above are now several years' old, and progress has been made since by these and other ANSPs. Unfortunately, evidence from trials and operation is not usually published, and not always even documented, and is dispersed between the various stakeholders. However it is suggested that it would be worthwhile (continuing to) update the knowledge of what systems are already being implemented, and to collate this systematically as Evidence. Without such up-to-date knowledge there is a risk of repeating work that has already been done. The intents and definitions of systems that have been implemented are not exactly the same as for FASTI, so the relevance of such evidence needs careful review.

Safety Issue: Further evidence that FASTI can operate over the full range of normal operational conditions should be sought from ANSPs who are already implementing FASTI-like tools. This evidence should then be collated and reviewed in order to extract from it evidence and lessons learned relevant to FASTI

Simulation evidence

The theoretical and practical evidence noted above is incomplete, and will probably remain so even after collating more up-to-date information from ANSPs. Further work will therefore be required. Adequate Fast Time and Real Time Simulations (FTS/ RTS) are the key to demonstrating acceptable safety performance at the pre-operational stage.

Simulation is particularly important in checking for emergent effects that result from the system-level interactions between the various elements, both steady-state and dynamic. Emergent effects are unlikely to be revealed by desk analyses.

The context and plans for simulations were set out in the Validation Plan [Ref.22] in Dec 2006. This now requires an update.

Safety Issue: An update on the Validation Plan is required, defining suitable safety metrics and planning what is to be simulated in order to ensure that safety aspects are sufficiently explored.

Safety Recommendations

The Validation Plan must include a definition of simulation objectives and appropriate and practical metrics for each. There is often a compromise between what should ideally be measured as the best indicator of safety and what is practical, because of limitations of simulation time or measurement techniques, and because of the limits on the veracity and fidelity of the simulation. It is therefore usual to have a range of metrics, with different strengths and weaknesses. Table 4 suggests objectives for the simulations, the reasons for including them and comments on practical metrics and methods of measurement.

Table 4: Simulation objectives and safety metrics

Objective/ Key parameters	**Rationale for inclusion**	**Metrics and methods for measurement**
Increase in proportion of conflicts detected and resolved at Planning stage	Key functionality and performance parameter as identified in Arg 1.1.6	
Increase in proportion of non-conformances detected and resolved at Planning stage	Key functionality and performance parameter as identified in Arg 1.1.6	
Effectiveness with which controllers keep Flight Plans up to date.	Key functionality and performance parameter as identified in Arg 1.1.6	Observation, controller debriefs, analysis of incidents where FP has not been updated. Controller errors in data input could also be measured

Objective/ Key parameters	Rationale for inclusion	Metrics and methods for measurement
Controller workload for a given traffic level	FASTI should reduce workload per aircraft handled by supporting monitoring for conflicts / non-conformances and CORT. Measurements are required to confirm that this is the case.	There are many ways to measure workload, mostly relatively straightforward, but the exact definition and interpretation of 'workload' are the subject of debate, with an extensive literature on the topic. Common measures are self-assessment ranking schemes such as Instantaneous Self Assessment (ISA) or post-run questionnaires such as NASA TLX. Physiological measurements such as heart rate are also used as a measure of workload/ stress. Workload should be measured as an average over the shift and also in terms of how often and how severely overloads occur.
Usability of the tools	Fundamental HF issue – feedback from users will be required to refine the HMI	Semi-structured questionnaires and/ or debrief scripts need to be designed
Tuning MONA and MTCD detection/ alert thresholds and procedures to harmonise with those of other conflict tools and safety nets such as TCT, STCA and TCAS		
Impacts of FASTI on PC/ TC interaction and communication		Observation, transcript analysis, debriefs
Effects of controller reaction times on effectiveness of the tools		
Frequency of STCAs, and other incidents, especially those related to PC vigilance.	Important to assess whether and how FASTI-related changes in working practices and cognitive activity may affect other safety occurrences	

Objective/ Key parameters	Rationale for inclusion	Metrics and methods for measurement
Balance between spurious alerts and failure to detect real conflicts/ non-conformances.	Too many spurious alerts distract the controller and may destroy trust in the tools. Failure to detect real events also destroys trust and may also be a direct safety hazard. In general, there is a trade-off between these, as they both depend on the sensitivity of the detection system. Simulation provides an opportunity to vary the sensitivity and hence optimise the balance.	The balance will depend principally on the tuning of the alert thresholds in MTCD and MONA, the accuracy of TP and the data provided to it, and the procedures for controller response to alerts . The rate of spurious alerts or failures could be recorded by the controllers. The optimum balance could be elicited through structured controller questionnaires and debriefs, or assessed more objectively by recording the workload, stress etc with different settings.

Guidance: ANSPs should carry out high-fidelity, site-specific RTSs of the functionality and performance of their specific FASTI concepts and designs. EUROCONTROL can carry out simulations for some typical situations, but it will not be adequate simply to combine the results of these with site acceptance testing of the tools. The RTSs should be dynamic as well as steady-state. Particular site-specific issues include the level of automation,

Conclusion for Arg 1.3

The evidence for correct and coherent functioning of the FASTI system over the full range of normal operational conditions is, currently, partial.

Suitable ranges of values for the parameters that define operational conditions will need to be decided on for simulation. It would be impracticable to test every possible combination that might affect FASTI, but the aim should be to test FASTI under a range of conditions that typify the range encountered in implementing centres.

High-level data flows between system elements should be analysed, hence identifying any additional Safety Requirements for internal coherence that may be required. Having done this, EUROCONTROL should decide how much further to go in defining the detail of information flows between system elements *Arg 1.3.2.*

A walk-through analysis of various scenarios should be performed in order to consider correct functioning of each element in the Logical Model.

Further evidence of correctness and coherence should be sought from theoretical analyses and from the experience of ANSPs who have already developed or implemented FASTI-like tools. It will also be essential to gather evidence from simulation, as EUROCONTROL indeed plans to do.

The first step is to update the Validation Plan to ensure that the simulations are designed to explore safety aspects adequately.

4.4 Arg 1.4: The FASTI high-level design is robust against external abnormalities

Aim and Strategy:

The argument is that the high-level design is robust against abnormalities in external ATM systems and the wider environment that may interact with FASTI.

The term 'abnormalities' includes both specific failures and errors and more general 'unusual conditions'.

Arg 1.4 has been broken down into two sub-arguments dealing, respectively, with the identification and assessment of abnormalities.

Arg 1.4.1 *Abnormalities in external systems have been identified*

Evidence:

The systems that have specific interfaces with FASTI were identified in the Logical Model (Figure 4) and in Arg 1.2.3. Assumptions have been made about the functionality, performance, reliability and integrity of these systems (Arg 1.2.3). The present Argument is concerned with cases in which there are, nevertheless, abnormalities in these systems. These abnormalities can be categorised as:

- loss or corruption of FDPS;
- loss or corruption of surveillance systems;
- loss or corruption of meteorological data systems; and
- loss or corruption of CORT functions in adjacent sectors/ centres.

Additionally, there may be certain abnormal conditions in other ATM systems and in wider environment that do not normally interact with FASTI, but that could have 'knock-on' effects on safety. These can be categorised as:

- aircraft emergencies, e.g. reaction to ACAS Resolution Advisory (RA), depressurization, loss of control;
- loss of R/T contact with one or more aircraft;
- human errors by pilots (e.g. instruction misheard/ taken by wrong aircraft, instruction incorrectly acted upon, leading to level busts etc); and
- human errors by controllers in tasks unrelated to FASTI (e.g. controller does not instruct aircraft/ instruction given to wrong aircraft). (Controller errors in using FASTI tools and procedures are considered under Arg 1.5.)

Arg 1.4.2 *The system can react safely to all reasonably foreseeable abnormalities in external systems*

This argument looks for resilience: the ability of FASTI to carry on operating with acceptable safely during such events and to recover from them afterwards[6].

Evidence:

Table 5 below outlines how FASTI would be affected by abnormalities in interfacing systems and what would be required to provide the necessary resilience.

Table 5: FASTI response to abnormalities in interfacing systems and requirements for resilience.

Interfacing system	**Abnormality**	**How FASTI will respond**	**What would be required to provide necessary resilience**
FDPS	Loss	Loss of all FASTI functions (and others)	Fallback procedures – reversion to 'manual' process. Note that other non-FASTI systems may also be affected.
	Corruption	Incorrect outputs	Consistency / reality checks, detection and alerting
Surveillance	Loss	Loss of all FASTI functions (and radar picture)	Fallback procedures for radar failure. These should already be in place, as all surveillance-related systems will be lost, not just FASTI
	Corruption	Incorrect outputs	Consistency / reality checks, detection and alerting
Meteorological data	Loss	Loss of all FASTI functions	Fallback procedures – reversion to 'manual' process
	Corruption	Incorrect outputs	Consistency / reality checks, detection and alerting
CORT functions in adjacent sectors/ centres	Loss	Loss of SYSCO functions	Fallback procedures – reversion to baseline (telephone/OLDI) process
	Corruption	Incorrect outputs of SYSCO	Consistency / reality checks, detection and alerting

[6] Losses or corruption of interfacing external systems could in some cases be manifested as failures of the FASTI system, which are considered under Arg 1.5 and the associated FHA. For example, loss of the FDPS would result in the failure 'loss of FASTI functions', while corruption of surveillance information could *inter alia* result in 'failure to detect a conflict'. Mitigations against the effects of such external abnormalities can therefore be subsumed in the requirements for mitigation against the effects of internal failures of FASTI. These are identified under Arg 1.5, so no additional mitigation Safety Requirements need to be defined here in Arg 1.4. Arg 1.4 is concerned, rather, with ensuring that there are adequate measures to prevent external abnormalities leading to failures of FASTI.

By collating the resilience requirements above, the following Safety Requirements can be defined:

SR-FAS-10 Fallback procedures shall be defined for cases in which FASTI functions are unavailable

Guidance SR-FAS-10 above is also intended to cover cases in which FASTI functions become unavailable due to internal failure (see Arg 1.5.2). In designing fallbacks that are proportionate to the risk associated with such events, it will be necessary to take account of the total probability of a fallback being required: i.e. the sum of the probabilities resulting from both external abnormalities and internal failures

SR FAS- 11 Consistency/ reality checks, detection and alerting must be provided, wherever practicable, to inform the controller in the event that FASTI produces incorrect information. These checks should be automated as far as reasonably practicable. Where automated checking is impossible or impracticable, procedures must be defined, where appropriate, requiring controllers to check certain critical or indicator information at defined intervals or on defined occasions.

For abnormalities in external systems that do not normally have interfaces with FASTI, Table 6 outlines how FASTI would be affected by them and what would be required to provide the necessary resilience.

Table 6: FASTI response to abnormalities in other external systems and requirements for resilience.

Abnormality	**Effect on FASTI / how FASTI will respond**	**What would be required to provide necessary resilience**
Aircraft emergencies, e.g. reaction to ACAS Resolution Advisory, depressurization, loss of control	FASTI should detect resulting conflicts or non-conformances	No additional requirements
Loss of R/T contact with one or more aircraft	No direct effect	No additional requirements Fallback procedures for R/T failure should already be in place.
Loss of corruption of data sources to interfacing systems (e.g. failure of aircraft transponder)	Loss/ corruption of inputs (e.g. aircraft transponder failure leads to loss of surveillance data for the affected aircraft, so MONA and MTCD will be unable to function correctly in relation to affected aircraft	Consistency / reality checks, detection and alerting

Abnormality	Effect on FASTI / how FASTI will respond	What would be required to provide necessary resilience
Human errors by pilots (e.g. instruction misheard/ taken by wrong aircraft, instruction incorrectly acted upon, leading to level busts etc)	FASTI should detect any resulting conflicts or non-conformances	No additional requirements
Human errors by controllers in tasks unrelated to FASTI (e.g. controller does not instruct aircraft/ instruction given to wrong aircraft).	FASTI should detect resulting conflicts or non-conformances	No additional requirements

From the above, one additional Safety Requirement has been defined.[7].

SR-FAS-12 FASTI shall provide an alert to the controller if any data sources become unavailable or (detectably) corrupted

To provide greater assurance that FASTI is robust against abnormalities in interfacing and external systems, and that fallback procedures are adequate, it is suggested that certain abnormalities should be simulated, although the limits on what can be realistically simulated need to be acknowledged

Safety Issue: Where appropriate, and so far as reasonably practicable, abnormalities in interfacing and external systems should be simulated in order to test the robustness of FASTI and prove the adequacy of fallbacks

ANSPs will need to identify and assess abnormalities in interfacing and other external systems at a more detailed, implementation-specific level, taking account of the specifics of the interfacing systems and the detailed design of their interfaces with FASTI.

Guidance: ANSPs should hold safety workshops (as described in the SAM) and make use of historic experience to identify abnormalities in interfacing and other external systems, assess the risks (frequencies of occurrence, and probabilities and severities of outcome) associated with them and hence refine or define additional Safety Requirements if necessary. As the interfacing systems support other ATM functions, not just those associated with FASTI, it may be that these Safety Requirements are already in place. Where appropriate and practicable, the effects of such failures should be investigated by simulation.

[7] It should be recalled (as described in Section 2.4) that FASTI is designed not merely to be robust against external abnormalities but to provides a safety benefit in relation to many abnormalities. This is because it should lead to a more conflict-free traffic pattern in which there is greater margin for error and more time to react, as well as supporting controllers in detecting and resolving any conflicts that arise as a result.

Conclusion for Arg 1.4

Safety Requirements have been defined to provide resilience in the event of abnormalities in interfacing external systems. To provide greater assurance that these will be effective in practice, EUROCONTROL should test the robustness of FASTI and the adequacy of fallbacks in simulations, where appropriate and practicable.

4.5 Arg 1.5 - Risk from internal failures is sufficiently reduced

Aim and Strategy

Unlike Arguments 1.1 to 1.4, which lead to a specification of the risk-reducing properties of FASTI (i.e. functionality and performance requirements) Argument 1.5 leads mainly to the specification of requirements on the reliability or integrity of FASTI.

Arg 1.5 has been broken down into two sub-arguments dealing, respectively, with the identification of internal failures and errors, and the definition of appropriate and proportionate Safety Requirements to reduce the associated risk.

Arg 1.5.1 *Failures within FASTI have been comprehensively identified*

Evidence:

A number of complementary methods have been applied to identify (and assess) failures (equipment failures, procedural failures or human errors) within the FASTI system. A FHA/PSSA was performed, in accordance with the EUROCONTROL SAM [Ref 3], to the extent possible at this stage in concept and high-level design. A Human Reliability Assessment (HRA) was performed using the EUROCONTROL methodology described in [Ref 30]. The findings of these studies incorporated failures identified in the hazard assessment workshop held within the Operational Focus Group (OFG) 7th meeting. [Ref.24] as well as material from EUROCONTROL working documents on FASTI and the FASTI CTA [Ref.16].

The collated log of failures, resulting hazards and Safety Requirements is presented in Appendix D.

Arg 1.5.2 *Safety Requirements have been defined that prevent or mitigate against the results of each failure, and that are proportionate to the level of risk*

Evidence:

Risks related to internal failures have been assessed within the failure log (Appendix D) and Safety Requirements have been defined accordingly. They are presented below under three sub-arguments, concerned with the prevention of internal failures (Arg 1.5.2.1), the mitigation of their effects (Arg 1.5.2.2) and fallback provisions, outside of FASTI, for use in the event that FASTI fails completely (Arg 1.5.2.3)

Arg 1.5.2.1 *Safety Requirements have been defined for prevention of internal failure*

Because failures of FASTI can have safety effects, the functions need to be of high reliability and integrity.

It is not possible to set quantitative targets at this stage, but the following Safety Requirement summarises the findings in Appendix D by presenting a list of failures, ranked in descending order of the severity of the effects of hazards that may result, and hence in descending order of the required reliability/ integrity.

SR-FAS- 13 The functions of FASTI need to be of high reliability and integrity. The following is an initial list of potential failures, ranked in descending order of severity of the effects of hazards that may result, and hence in descending order of the reliability/ integrity demanded of the related functions.

HIGHEST SEVERITY/ HIGHEST DEMAND ON RELIABILITY/ INTEGRITY

- Failure to detect genuine conflict/ or non-conformance
- Loss of all or some FASTI functions
- Incorrect or inaccurate information provided by tools

MEDIUM SEVERITY/ DEMAND ON RELIABILITY/ INTEGRITY

- Controller does not notice conflict/ non-conformance alert
  Controller does not monitor concerned aircraft
- Display of wrong information about a conflict/ non-conformance - eg shows minimum distance as 3NM when in reality it will be 1 NM
- Display of wrong conflict/ non-conformance type (e.g. wrong conflict geometry, level bust rather than track deviation)
- Only one conflict for an aircraft when actually there are two or more (failure to correlate conflicts)
- Loss or corruption of CORT information, or information addressed to wrong sector (includes message set not same for inter-sector and inter-centre CORT)
- Reminder presented too early/ too late
- Reminder content incorrect (e.g. 'Turn HDG 230' rather than 'Turn HDG 270')
- What-if probing provides misleading information regarding the edited trajectory – e.g. shows proposed resolution to be conflict-free when it is not (e.g. due to failure to identify aircraft constraining the resolution)
- PC transfers conflicts/ non-conformances to TC at inappropriate time
- PC sets inappropriate thresholds for automatic transfer to TC.
- Controller does not update system, or enters incorrect information
- Clutter - too many conflicts/non-conformances or too much info on each conflict/ non-conformance
- Controller wrongly ignores an alert (sees it as of low significance) For example controllers may currently be more inclined to look for conflicts than FL deviations, as the latter can be difficult to detect. They may persist with this strategy and so not place much importance on MONA warnings, and hence not obtain the benefit
- Controller misinterprets alert information (e.g. confuses objects selected, misreads numbers…)

- Controller forgets or loses awareness of mode/ settings (e.g. thinks a lower threshold is in use, or that lookahead is further than it is)
- Automatic transfer of conflicts to TC is too late, or not at all
- Trajectories not updated correctly
- Controller sending message makes error in entering data or addressing the message
- Controller overloaded with CORT messages. Several communication lines could be open at the same time. The messages will not in themselves convey the sense of relative urgency/ priority that can be given in telephone conversation
- CORT requests not answered in time or message and response misordered. Note that messages may be sent simultaneously or cross in transit
- Over-reliance on tools

LOWEST SEVERITY/ LOWEST DEMAND ON RELIABILITY/ INTEGRITY

- Spurious indication of non-existent conflict/non-conformance
  This may apply to single or multiple problems, or to the special case of conflict/non-conformance that has been resolved but is still showing
- System prioritization of conflicts/ non-conformances is misleading (wrong)
- Controller does not verify problem with concerned aircraft
- Spurious constraint on resolution identified
- Automatic transfer of conflicts/non-conformances to TC is too early (i.e. before the threshold established by the PC)
- Incoming coordination/ transfer messages not noticed
- Under-reliance on tools

Guidance: ANSPs will need to review and expand on the above list in their own FHA/PSSA process.

Guidance: High reliability and integrity of FASTI functions were also a Safety Requirement (SR-FAS-03) under Arg 1.2.2. This is because FASTI needs to be dependable in order to maximise the safety benefits of its success as well as to minimise the risks associated with failure. As the detailed design emerges, and reliability and integrity targets can be quantified or ranked more robustly, it will be necessary to consider the demands of both the success and failure cases, and set targets on each function that will satisfy the more stringent demand in each case.

Arg 1.5.2.2 *Safety Requirements have been defined to mitigate the effects of internal failure*

The following SRs define measures within FASTI itself that can mitigate against the effect of internal failures.

SR-MTCD-10 MTCD shall, where appropriate, give a warning to the controller if no response is received to a conflict alert within a certain time.

SR-MONA-09 MONA shall, where appropriate, give a warning to the controller if no response is received to a non-conformance alert within a certain time.

SR-FAS-14 FASTI shall provide a self-diagnostic alert to the controller if any of the component tools (MTCD, MONA or SYSCO) become unavailable or unreliable.

SR-HMI-10 The HMI shall alert the controller if any conflicts are not visible on the display (e.g. if using a zoomed-in view, or because of filtering of certain traffic)

SR-HMI-11 The HMI shall alert the controller in the event of an incorrect response or attempt to use a tool inappropriately, where this is detectable (e.g. incorrect syntax of SYSCO message)

To provide greater assurance that these 'in principle' benefits are realised in the complexities of practical ATM, it is suggested that certain internal failures should be simulated, although the limits on what can be realistically simulated need to be acknowledged

Safety Issue: Where appropriate, and so far as reasonably practicable, internal failures should be simulated,

Other, more implementation-specific internal failures will need to be identified and assessed by ANSPs, taking account of the specifics of their designs.

Guidance: ANSPs should carry out FHA/ PSSA (as described in the SAM) to identify internal failures and errors in their specific implementation of FASTI, to assess the risks they present and hence to refine or define additional Safety Requirements. Where appropriate and practicable, the effects of such failures should be investigated by simulation.

Arg 1.5.2.1 *Safety Requirements have been defined for fallback in the event that FASTI fails completely*

SR-FAS-10 Fallback provisions shall be defined for cases in which FASTI functions are unavailable

Guidance SR-FAS-10 above has already been stated in Arg 1.4.2, as it is also intended to cover cases in which FASTI functions become unavailable due to external abnormalities. In designing fallbacks that are proportionate to the risk associated with such events, it will be necessary to take account of the total probability of a fallback being required: i.e. the

sum of the probabilities resulting from both external abnormalities and internal failures.

Guidance: Note that, by definition, fallback measures are outside the FASTI system and therefore have to be defined by ANSPs – they may include for example back up systems or reversion to 'manual' procedures

Conclusion for Arg 1.5

Safety Requirements have been defined to make the FASTI high-level design acceptably safe despite the potential for internal failures. To provide greater assurance that this will be true in practice, EUROCONTROL should test the effects of internal failures in simulations, where appropriate and practicable.

4.6 Arg 1.6 - Suitability and sufficiency of the safety assessment

Aim

This is a backing argument, showing that the safety assessment process has been suitable and sufficient.

Evidence

The PSC has been developed in accordance with the EUROCONTROL SCDM and SAM. It has also been informed by more recent good practice guidelines and experience from other studies, in particular by using the EUROCONTROL Generic Safety Argument and SAME guidelines [Ref.15]. This has helped to make use of lessons learned on other studies. Also, because the SAME guidelines should become increasingly familiar to stakeholders (Safety Case developers, users, auditors and regulators) it will facilitate development, review and audit of the full Safety Cases by ANSPs.

The team that produced this PSC has many years' experience in all the key areas of safety assessment and management and in Safety Case development, both in ATM and opther domains. They also have specialist expertise in ATM operations, human factors and system development.

Safety Issue: It would be desirable to have more input from ANSPs in ongoing work. This will ensure that practical issues are not missed and that the final issues of the PSC and accompanying Guidance document are as useful as possible to ANSPs.

Conclusion for Arg 1.6

This PSC has been developed using a sound safety assessment process, consistent with the EUROCONTROL good practice guidance, by people with appropriate skills and experience. However, further input from ANSPs will be desirable, to ensure that the final issue of the PSC and associated guidance are as practical and useful as possible.

4.7 Arg 1.7 - All Safety Requirements are realistic and demonstrable

This argument aims to show that the Definition of FASTI, and in particular the Safety Requirements, is realistic – i.e. that it is feasible to satisfy the Requirements in a typical implementation in hardware, software, people and procedures. It also aims to show that it will be possible to demonstrate that Safety Requirements have been achieved.

Evidence

The OFG meetings and other external workshops and presentations continue to provide a forum for stakeholders to express ideas about the feasibility of implementing FASTI safely. None of the Safety Requirements identified to date appears overly demanding in terms of available knowledge, technologies or human performance.

Further evidence that the Requirements are realistic is provided by having outlined credible approaches to the Safety Arguments for later stages of the system lifecycle (Args 2, 3 and 4) as described in Section 5 following.

Safety Issue The realism of what is expected from implementing ANSPs, through the Safety Requirements, is subject to the continuing involvement of stakeholders in the safety process. Hence, as in Arg 1.6, it would be desirable to involve ANSPs more closely in ongoing work within EUROCONTROL.

Guidance: For some Safety Requirements it is difficult to show conclusively whether or not they have been satisfied - satisfaction is often a matters of degree rather than a simple binary (yes/no) question.

Demonstration that SRs have been achieved can be a major problem for ANSPs, due to the limited ability of the available, test-based validation & verification methods to show, with sufficient confidence, that the Safety Requirements have actually been satisfied in practice.

To work around this problem, the Assurance Level process [Ref.15] can be used to define the rigour of the process that must be followed to implement the Requirements. It provides a method of deciding how much Evidence is enough, and what activities should be carried out to ensure this. The Assurance Level process is described further in Argument 2.1 and is illustrated in the Guidance [Ref 1].

Conclusion to Arg 1.7

It is believed that the Definition and associated Safety Requirements are realistic - they would not place unreasonable expectations on implementers. However this is subject to the continuing involvement of stakeholders in the safety process.

5. COMPLETING THE SAFETY CASE: IMPLEMENTATION, TRANSITION AND OPERATION (ARGS 2,3,4)

This PSC is principally concerned with demonstrating the safety of the FASTI concept and high-level design, i.e. with EUROCONTROL's responsibilities. ANSPs are responsible for demonstrating safety of the later stages in the lifecycle. Nevertheless, this Section outlines possible argument structures for those later stages, in order to provide confidence that these stages will be feasible (supporting Arg 1.7) and to provide, in conjunction with the Guidance Document [Ref.1], a starting point for ANSPs developing full Safety Cases.

The material presented here draws on the FASTI Good Practice in Implementation Guidelines [Ref 21] and the EEC Transition guidelines [Ref 22].

For each Argument, we expand on what it involves (where additional detail is required beyond that in the Argument title), and outline how that could be achieved.

ANSPs will need to build upon these Arguments and provide the Evidence to support claims that their implementation, transition and operation of FASTI is safe. Consequently, no Evidence can be given for these Arguments at this PSC stage. However, the types of Evidence that may be needed are outlined, where possible, within the Guidance. Further detail of what Evidence will be needed and how it may be gathered will be provided in the separate Guidance Document [Ref 1].

It is essential that implementation, transition and operation are conducted under a suitable Safety Management System, including the development of an implementation plan and appropriate risk assessments. This PSC covers the specifics of FASTI, not general considerations of ATM safety management.

5.1 Safety of FASTI Implementation (Arg 2)

Aim and Strategy

Arg 2 is concerned with the safety of the implementation of FASTI, in which the definition 'on paper' is built into an actual system of physical hardware, software, trained people and written procedures. It aims to establish whether the physical system as built achieves the required level of safety.

Arg 2 has been broken down into sub-arguments covering the incorporation of the Safety Requirements from the Definition into the detailed design (Arg 2.1), the possibility that new hazards are introduced as emergent properties when the system elements are combined (Arg 2.2) and then arguments that the practical processes of feasibility studies procurement, construction, integration and commissioning are performed safely (Args 2.3 – 2.7).

Arg 2.1 *All Safety Requirements identified in the Definition have been incorporated in the detailed design*

This Argument needs to show that all Arguments and Evidence related to the Definition (i.e. Arg 1 as detailed in Section 4 of this PSC) have been actively reviewed, and developed or amended as necessary for the specific context, and included in the detailed design.

By formalising the concept and design intent as Requirements: i.e. in a way that can form a clear basis for procurement, this argument is important in preventing 'requirements creep' - the gradual compromising or downgrading of intended benefits.

It is at this stage that the ANSPs often encounter a major problem: the limited ability of the available, test-based validation & verification methods to show, with sufficient confidence, that the Safety Requirements have actually been satisfied in practice. This is especially a problem for reliability / integrity SRs, in that ideally one would wish to prove that failures do not occur more frequently than their allowable, often extremely low, target levels. It is also a problem where SRs cannot be expressed in ways that allow a simple yes/no response but are, rather, matters of degree. (Such SRs are not ideal, but sometimes unavoidable.)

To address this problem the EUROCONTROL SAM Task Force has been developing an assurance-based approach as a pragmatic (albeit somewhat indirect) means of demonstrating the satisfaction of Safety Integrity Requirements (and in some cases, Functional Safety Requirements) [Ref 15].

This approach is based on the assignment of assurance levels (ALs), determined by the safety-criticality of the system element concerned, and which themselves determine the related assurance process in the form of objectives, activities and evidence requirements.

It is important to note that ALs do not replace Safety Requirements; rather, they set the level of assurance at which satisfaction of Safety Requirements has to be demonstrated

Arg 2.2 *Nothing in the process of implementation has introduced additional risks*

When system elements are combined and begin to interact, it is possible that new hazards may arise, as emergent properties. It is necessary therefore to consider the system as a whole.

Simulations, including dynamic simulations, should be performed to check the safety of the whole system in practice and identify emergent properties. However it may be more efficient and effective if this is carried out once the system is fully implemented and ready for Transition (Arg 3.1). Bottom-up analytical techniques such as HAZOP or FMEA may also help in looking for potential common cause failures.

ANSPs will need to look for and mitigate against common cause failures in their implementations.

Arg 2.3 *Selection of the various possible physical implementation options has been carried out with sufficient regard to safety*

Feasibility studies and option selection need to consider safety aspects thoroughly. The process and findings should be captured in an updated Safety Argument and Safety Case. The selection of options should have regard to the satisfaction of **Cr02** - does the chosen option minimise risk?

Arg 2.4 *Procurement has been carried out with sufficient regard to safety*

ANSPs should check that all relevant SRs are clearly written into tenders and contracts with suppliers. Any changes to or variations from specifications need to be fed back to those responsible for safety and the implications for the Safety Case assessed before the changes are accepted .

Arg 2.5 *Detailed design has been carried out with sufficient regard to safety*

Safety Requirements for design under Args 1.2 - 1.5 should be developed and extended where necessary and checked off as they are implemented. developing metrics for and thresholds of acceptability for each interfacing. For example, it will be necessary to tune the MTCD / MONA thresholds to local needs and context,

Arg 2.6 *Construction/ integration has been carried out with sufficient regard to safety*

This stage include manufacture of hardware, writing software, writing detailed procedures etc.

Any changes to/ variations from specifications during construction/ integration need to be fed back to those responsible for safety and the implications for the Safety Case assessed.

The Operations Manual and associated Procedures should be written at this stage (and indeed should have been defined in outline at the concept stage - Arg 1). Procedures should not be created to mitigate design deficiencies discovered at a late stage. Activities required will depend on degree of control over, and trust in, subcontractors and suppliers and their QA processes

Arg 2.7 *Commissioning has been carried out with sufficient regard to safety*

It is not sufficient for ANSPs to rely on standard site acceptance testing, as this will not identify any issues that arise under unusual conditions. Nor is it adequate to rely on type approval of Equipment - as this cannot take account of the widely varying ways of using the tools and their contexts of use. Pre-operational simulations (see Arg 3.1) will be required.

5.2 Safety of FASTI Transition (Arg 3)

Aim and Strategy

This argument aims to show that transition from the old to the new system is performed safely.

Arg 3 has been broken down into sub-arguments covering: bringing the existing system up to the baseline if necessary (Arg 3.1) pre-operational simulation (Arg 3.2), hazards in the transition process itself (Arg 3.3) and then arguments that the practical processes of final preparation for operation (Args 3.4 – 3.9).

Arg 3.1 *The existing system has been safely brought up to the baseline*

Actual pre-FASTI situations will vary across ANSPs and States. For the purposes of this PSC, a 'typical' baseline pre-FASTI situation has been defined (as described in Appendix C) . If an ANSP starts from a different baseline, they will need to adapt and develop their Safety Case accordingly. For example, if an ANSP needs to implement some enabling measures to come up to the baseline, they would need a Safety Case covering those enablers as well as the baseline-to-FASTI changes.

Arg 3.2 *Pre-operational validation has been carried out*

ANSPs should conduct pre-operational simulations and user trials, including dynamic simulations, to check safety in practice and identify emergent properties. This should include effects on neighbouring, non-FASTI airspace.

Arg 3.3 *Nothing in the Transition process has introduced additional risk*

All hazards associated with switch-over from the old systems to the new systems must be assessed and mitigated sufficiently. ANSPs should carry out hazard identification and risk assessment studies to look for potential failures and errors in transition. Examples could include incorrect re-wiring when swapping over from old to new hardware, or effects of increased capacity within the FASTI airspace on downstream sectors.

Arg 3.4 *Safety-related training has been achieved*

This argument must cover training of operational controllers in normal operation, for emergencies, abnormal and degraded modes and contingencies. It should also include consideration of any implications for the training of On-Job Training Instructors, Watch Supervisors, and *ab initio* trainees.

It is important to ensure understanding of basis and intent of FASTI tools as well as practical 'how to' instruction. This will support correct expectations and use of tools - eg in the importance of updating the system.

Ensure that training sets up appropriate expectations of the tools and degree of trust. Refer here to the EUROCONTROL Human Factors

Case approach [Refs 26, 27, 28, 29] and the SHAPE project [Ref 31] which gives guidance on training to build up trust

Take account of controllers being trained on new system but still having the mindset relating to the old one, or of interference from the old mindset.

Be aware of danger of training on the system before it is stable.

Arg 3.5 *Working methods are safe and appropriate*

ANSPs should review whether TC and PC working methods are well-matched – for example in speed of working, competencies required and PC/ TC expectations of each other when TC is using TCT. These matters should have been considered already in reviewing Arg 1 and in Arg 2 – in Transition the intentions and assumptions need to be updated.

Arg 3.6 *Procedures and other required documents and resources are readily available to users and stakeholders*

ANSPs should carry out final tests and refinement of the Ops Manual and Procedures with users.

ANSPs should consider making Procedures available on Intranet, to assist dissemination for review and accessibility, as well as in hard copy form in the Operations Room.

The preparations should also include publication of operational procedures, airspace changes (if any), publication of engineering procedures, provision of resources (people, equipment spares, maintenance facilities etc)

The process of switching over from the old systems to the new systems has been fully planned and resourced. This should include switchover procedures, allocation of responsibilities and the training / briefing of all personnel involved.

Arg 3.7 *Shadow-mode operations have established safety in a realistic operational context*

ANSPs should monitor user acceptance and adaptation to new practices, roles, teamwork, adherence to procedures, and modify system or training if required.

Arg 3.8 *Pre-FASTI systems has been safely removed (or left in place as fallback*

Systems that will no longer be required should be safely removed. This includes, for example, uninstalling software. As appropriate, some old systems may need to be left in place as fallback, with associated procedures accessible and trained for.

Arg 3.9 *O-date itself and initial operations safely carried out.*

5.3 Safety of FASTI Operation (Arg 4)

Aim and Strategy

Arg 4 aims to show that the operational use of the system, including its maintenance and updating, will continue to be acceptably safe. Arg 4 is broken down into four sub-arguments as follows:

Arg 4.1 *Post O-date monitoring and feedback continue to ensure safety in operation*

Post O-date monitoring and feedback will be required, especially to establish the ongoing safety of for aspects that can only realistically be checked in operational service. Key aspects to include are:

- Reporting system in place for controllers to report any difficulties.
- Training instructor available in early days of operation
- Monitoring of incidents and safety metrics (re-use, with adaptation if required, the metrics defined for use in simulation in Arg 1.3.3)
- Monitor and / or set up feedback schemes for usability, workload, roles, teamwork - in general how controllers are adapting to new work methods. Are they as expected? Do real work practices match written procedures?
- Monitor MTCD alerts – for example identifying sectors that have more conflicts than others, trends over time. Monitor more generally for unexpected emergent effects or uses beyond intent.
- Feedback may be expected especially regarding tuning of system parameters (eg to optimise false alert rate) and training ('what you wish you had known')

Arg 4.2 *Maintenance and upgrades/ updates are safely performed*

ANSPs should ensure that adequate budget and human resources are available for further simulations or re-training in event of significant upgrades/ updates

Refresher training should be conduced at sufficiently frequent intervals (including reversion to 'manual' methods in event that FASTI is unavailable)

Arg 4.3 *Changes in the operational environment are identified and responded to*

ANSPs should monitor changes in the external environment that may affect design basis assumptions. Consider for example changes in traffic, airspace, introduction other new systems. This should be part of the ANSP's wider SMS, providing for regular monitoring and review of changes

Arg 4.4 *FASTI is safely decommissioned at the end of its life*

This is outside the scope of FASTI, in that any safety issues should be identified in the Safety Case process for the *new* system, assuming that the SMS is operating properly. However, future problems can be avoided by ensuring that documentation explaining the 'what' and 'why' of FASTI, i.e. the design and its rationale as covered in Arg 1, is adequate and readily available.

6. ASSUMPTIONS, ISSUES AND LIMITATIONS

This section summarises the assumptions and outstanding issues in the present PSC, and any limitations on the operation of FASTI that are currently seen to be necessary

6.1 Assumptions

The main assumption on which the PSC relies (**A01**) is that current (baseline) operations are acceptably safe. For most ANSPs, and for ECAC airspace as a whole, this will probably remain an assumption for some time, given the complexity of trying to apply formal safety assessment and risk tolerability methods to the whole of ATM, although EUROCONTROL is working on the issue [Ref.23].

It is assumed that interfacing systems: the FDPS (**A02**), surveillance systems (**A03**) and meteorological data systems (**A04**) are of sufficiently high functionality, performance, reliability and integrity to provide the information needed by FASTI accurately, dependably and in good time.

It is also assumed that adjacent centres, especially those that are not FASTI-equipped, will review and where necessary adapt and agree revised co-ordination and transfer procedures and LOAs to accommodate any changes needed for FASTI (**A05**).

6.2 Safety Issues

The present PSC is a living document, and the following Safety Issues will need to be resolved before it can be finalised. The Argument numbers to which these issues relate are given for traceability.

- The FASTI Operational Concept needs to be developed to identify and address, comprehensively, issues relating to interfaces with and impacts on neighbouring non-FASTI airspace*. Arg 1.1.4*
- EUROCONTROL should consider whether it may be possible to define example thresholds of acceptability for the key functionality and performance and parameters, for a typical implementation. *Arg 1.1.6*
- The nature and extent of changes in working practices and cognitive activities resulting from FASTI need to be identified more robustly (e.g. by simulation), and their effects on safety assessed. *Arg 1.2.1.4*
- Suitable ranges of values for the parameters that define operational conditions will need to be decided on for simulation. It would be impracticable to test every possible combination that might affect FASTI, but the aim should be to test FASTI under a range of conditions that typify the range encountered in implementing centres. *Arg 1.3.1.*
- High-level data flows between system elements should be analysed, hence identifying any additional Safety Requirements for internal coherence that may be required. Having done this, EUROCONTROL

should decide how much further to go in defining the detail of information flows between system elements *Arg 1.3.2.*

- A walk-through analysis of various scenarios should be performed in order to consider correct functioning of each element in the Logical Model. *Arg 1.3.3*
- Further evidence that FASTI can operate over the full range of normal operational conditions should be sought from ANSPs who are already implementing FASTI-like tools. This evidence should then be collated and reviewed in order to extract from it evidence and lessons learned relevant to FASTI. *Arg 1.3.3*
- An update on the Validation Plan is required defining suitable safety metrics and planning what is to be simulated in FTS/ RTS to ensure that safety aspects are sufficiently explored. *Arg 1.3.3*
- Where appropriate, and so far as reasonably practicable, abnormalities in interfacing and external systems should be simulated. In order to test the robustness of FASTI and the adequacy of fallbacks. *Arg 1.4.2*
- Where appropriate, and so far as reasonably practicable, internal failures should be simulated. *Arg 1.5.2.2*
- It would be desirable to have more input from ANSPs in ongoing work. This will ensure that practical issues are not missed and that the final issues of the PSC and accompanying Guidance document are as useful as possible to ANSPs. *Arg 1.6*
- The realism of what is expected from implementing ANSPs, through the Safety Requirements, is subject to the continuing involvement of stakeholders in the safety process. Hence, as in Arg 1.6, it would be desirable to involve ANSPs more closely in ongoing work. *Arg 1.7*

6.3 Limitations

No limitations on the deployment of FASTI have been identified to date, beyond those inherent in the design intent and Operational Concept. The concept and high-level design appear potentially appropriate for any ECAC en-route airspace.

7. CONCLUSIONS

With regard to the overall claim that FASTI will be safe for operational use, this PSC has shown that the FASTI concept and high-level design can satisfy this claim in the proposed operational context.

A number of Safety Issues remain to be addressed before this claim can be fully substantiated and the PSC finalised, but none of these are seen as being particularly difficult to resolve in principle. The main needs for the future are to ensure that adequate ANSP input is obtained, and that appropriate simulations are carried out.

APPENDIX A: ABBREVIATIONS

ABI	Advance Boundary Information (OLDI message)
ACAS	Airborne Collision Avoidance System
ACC	Area Control Centre
ACT	Activation Message (OLDI)
AFARP	As Far As Reasonably Practicable
ANSP	Air Navigation Service Provider
ATC	Air Traffic Control
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATMSP	Air Traffic Management Service Provider
ATSU	Air Traffic Services Unit
BFD	Basic Flight Data message
CFD	Change to Flight Data message
CM	Capacity Management
CORT	Co-ordination and Transfer
CTA	Cognitive Task Analysis
EATMP	European Air Traffic Management Programme
ECAC	European Civil Aviation Conference
EEC	EUROCONTROL Experimental Centre
ERATO	En-route Air Traffic Organiser
ESARR	EUROCONTROL Safety Regulatory Requirement
ETMA	Extended Terminal Movement Area
FASTI	First ATC Support Tools Implementation
FDPS	Flight Data Processing System
FHA	Functional Hazard Assessment
FLAS	Flight Level Allocation Scheme
FM	Flow Management
FP	Flight Data
FSR	Functional Safety Requirement
FTS	Fast Time Simulation
GAT	General Air Traffic
GSA	Generic Safety Argument
HCI	Human Computer Interaction
HFC	Human Factors Case
HMI	Human-Machine Interface/ Interaction
HRA	Human Reliability Assessment
ISA	Instantaneous Self Assessment
LAM	Logical Acknowledgement Message (OLDI)

LOA	Letter Of Agreement
MAC	Message for the Abrogation of Co-ordination (OLDI)
MONA	Monitoring Aids
MSP	Multi Sector Planner
MTCD	Medium-Term Conflict Detection
MUAC	Maastricht Upper Area Control Centre
NATS	National Air Traffic Services (UK)
NM	Nautical Mile
OAT	Operational Air Traffic
OFG	Operational Focus Group
OLDI	On-Line Data Interchange
OSED	Operational Service and Environment Description
PC	Planner Controller
PSC	Preliminary Safety Case
PSSA	Preliminary System Safety Assessment
RA	(ACAS) Resolution Advisory
REV	Revision Message (OLDI)
RMC	RM Consultants Ltd
R/T	Radiotelephony
RTS	Real Time Simulation
SA	Situation Awareness
SAM	Safety Assessment Methodology (EUROCONTROL document)
SCD	Strategic Conflict Detection
SCDM	Safety Assessment Development Manual
SCR	Strategic Conflict Resolution
SIR	Safety Integrity Requirement
SME	Subject Matter Expert
SMS	Safety Management System
SR	Safety Requirements
STCA	Short Term Conflict Alert
SYSCO	System Supported Co-ordination
TC	Tactical Controller
TCAS	Traffic Alert and Collision Avoidance System
TCT	Tactical Controller Tool
TLX	Task Load Index
TMA	Terminal Manoeuvring Area
TP	Trajectory Prediction
TPU	Trajectory Prediction Update
TSA	Temporary Segregated Area

APPENDIX B: REFERENCES

1. EUROCONTROL. FASTI Safety Case Guidance Document - to be completed

2. EUROCONTROL. Safety Case Development Manual, Edition 2.2, 13 Nov 2006

3. EUROCONTROL. Air Navigation Safety Assessment Methodology (SAM) www.eurocontrol.int/safety/public/standard_page/samtf.html Edition 2.0

4. EUROCONTROL. ESARR4 - Risk Assessment in ATM, Edition 1.0, 5 Apr 2001.

5. EUROCONTROL. FASTI Operational Concept, Edition 1.1 (Working Draft), 20 Mar 2007

6. EUROCONTROL Experimental Centre, MTCD Concept of Operation, EATCHIP III Evaluation and Demonstration Phase 3A_Bis, Issued Sept 1999.

7. EUROCONTROL. MTCD Operational Service and Environment Description (OSED) Edition 0.4, Nov 2006

8. EUROCONTROL. MTCD Operational Requirements and Implementation Guidelines v2 2007

9. EUROCONTROL. MONA Operational Service and Environment Description Edition 0.2, June 2007

10. First ATC Support Tools Implementation Programme, Strategy for the Implementation of Enhanced Co-ordination and Transfer Facilities in Europe, Edition 3, 12th Jun 2006

11. EUROCONTROL, FASTI Operational Requirement for Trajectory Prediction – Volume 1 - The Planned and Tactical Trajectories, Edition 0.6, 14th Mar 2008.

12. ICAO Document 9854, Global Air Traffic Management

13. EUROCONTROL. Safety Policy dated Jan 2006.

14. EUROCONTROL. SRC Policy Doc 1, Edition 1.0, 14 Feb 2001.

15. Fowler D. Safety Assessment Made Easier. Part 1 - Safety Principles and an introduction to Safety Assessment. Edition 0.91 (Mature Draft), 29 Feb 2008. EUROCONTROL.

16. EUROCONTROL. FASTI – Cognitive Task Analysis. Edition 0.5, 9 July 2007

17. Norman D. The Design of Everyday Things, MIT Press, Fourth printing, 2001, ISBN 0-262-64037-6

18. EUROCONTROL. FASTI Baseline Description, Edition 1, 18 Sep 2006.

19. Beers, C. S., and Dehn, D.M. MTCD Shadow Mode Trials at Malmo Air Traffic Control Centre: Final Report. Amsterdam: National Aerospace Laboratory. 2002

20. Beers, C.S., and Dehn, D. M. MTCD Final Report: For Shadow Mode Trials at Rome Area Control Centre (ACC). Amsterdam: National Aerospace Laboratory. 2003

21. EUROCONTROL. FASTI - The Good Practice in Implementation study, Executive Summary, Edition Number 1.0, Working draft.

22. EUROCONTROL Experimental Centre. A Safe Approach to Transition: Key Elements for Transition Success, EEC Report No. 405, Oct 2006.

23. EUROCONTROL Experimental Centre. The Integrated Risk Picture Project for Air Traffic Management in Europe, April 2008.

24. EUROCONTROL. FASTI Medium Term Conflict Detection (MTCD) – Operational Hazard Assessment (OHA). Notes from FASTI OFG 7th meeting

25. EUROCONTROL. FASTI Validation Plan. Edition 1.0, Dec 2006

26. The Human Factors Case – Guidance for Human Factors Integration. EATM Infocentre Reference: 040201-08. August 2004. www.eurocontrol.int/eec/public/standard_page/human_factors_case.html

27. EUROCONTROL. The Human Factors Case: Managing Human Factors Issues for ATM Projects. Edition 1.4, 12 Feb 2007

28. First ATC Support Tools Implementation (FASTI) Human Factors and Managing the Transition Good Practice Guidelines, 21st June 2007.

29. First ATC Support Tools Implementation (FASTI) Human Factors Guidelines for MTCD, MONA and SYSCO, 21st June 2007.

30. EUROCONTROL. A Method for Predicting Human Error in ATM (HERA-PREDICT). Edition 1.0, 2004

31. EUROCONTROL SHAPE project, (Solution for Human Automation Partnership in European ATM), http://www.eurocontrol.int/humanfactors/public/standard_page/Shape_Overview_2.html

APPENDIX C PRE-FASTI BASELINE

The following information describes the assumed 'typical' system prior to FASTI implementation.

Flight Plan Information

In most existing systems flight plan information is displayed either:

- In the form of electronic flight bay (e.g. electronic flight strips) and is also available in the extended radar label. Normally, electronic strips are displayed on the PC position and the TC uses the flight plan information available in the radar label or
- In the form of paper flight strips.

TC – PC working methods

The Planning Controller:

- Shall scan for conflicts between all aircraft planned to enter the sector and, if the traffic situation allows, perform necessary coordination to ensure that aircraft entering sector are conflict free;
- Shall warn TC of any potential conflict between aircraft about to enter the sector or already inside the sector;
- Shall warn TC of any conflicts between aircraft about to enter the sector or already inside the sector and any active military areas;
- Shall assist the TC in conflict detection / resolution;
- Shall monitor the sector frequency and the progress of all flights within the sector and warn the TC of any potential tactical conflicts / unsafe clearances, if missed by TC.
- Shall ensure that entry / exit planning is in accordance with LoAs and perform necessary coordination;
- Ensure the correct transmission – reception of flight plan information and make any verbal coordination as appropriate;
- In a situation where ACT exchange is not affected, pass / receive verbal estimates to appropriate centre, and make appropriate inputs in the FDP system;
- Accept / transmit revisions, approval requests, expedite clearances and releases from / to adjacent centres and inform Tactical Controller accordingly;
- Update the system by entering flight profiles.

The Tactical Controller:

- Detect and solve conflicts between flights taking into account rules and procedures;
- Shall ensure that all aircraft within his sector are clear of any active military areas;

- Maintain continuous monitoring of flights and provide them with appropriate instruction in order to maintain separation or in order to ensure that all flights adhere to the given ATC clearance;

- Ensure that coordination is effected with appropriate centre regarding aircraft which are not separated in accordance with LoAs;

- Ensure that coordination is affected with military units in accordance with procedures specified in the LoAs;

- Ensure that before clearing an aircraft to another flight level, appropriate input has been made in order to update the system.

Conflict Detection

All flights entering or exiting a sector are subject to Flight Level Allocation Scheme (FLAS) and allocation of constraints (entry / exit flight level, routing, speed) in accordance with LoAs and other procedures. Based on these conditions / constraints, PC establishes and plans the traffic situation within the sector.

Most conflicts are solved by TC on tactical basis, 4-6 minutes ahead of the conflict.

Conflict detection / planning is done by scanning the radar screen, and using the relevant flight plan information (routing, aircraft type, requested flight level, destination).

Speed vectors and QDM are the tools used to assess the severity of the potential conflict within the sector.

As one of the main tasks of the PC is telephone coordination with neighbouring centres, the time left for planning of traffic in advance, potential traffic de – confliction and conflict resolution advice is limited.

Electronic Coordination

The following OLDI messages are available in most systems:

ABI – Advanced Boundary Information Message

ACT – Activation Message

LAM – Logical Acknowledgement Message

In a situation where the exchange of basic OLDI messages (ABI, ACT, LAM) is not available between ATC centres, verbal estimates have to be passed to / from appropriate centres.

Telephone coordination is effected by PC for the following types of coordination with adjacent / subsequent centres:

- Approval Requests

- Expedite Clearances

- Releases

- Revisions
- Estimates

Monitoring Aids

Most existing systems do not detect any deviation of aircraft from trajectory.

APPENDIX D INTERNAL FAILURES, RESULTING HAZARDS AND SAFETY REQUIREMENTS

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking (1 high to 5 low)**	**Safety Issues**	**Guidance for ANSPs**	**Safety Requirements**
Detect and Display Conflicts or Non-Conformances (NC) (including the monitoring and TP functions as well as the actual detection)	**Fail to detect genuine conflict/ NC** This may apply to single/ multiple conflicts. It may result from either failure to detect at all, or failure to do so in time.	U	Conflict or NC not detected for an unacceptable length of time.	2		Develop appropriate 'intelligence' of detection algorithms, with tuning to local operational context and needs. Further research is required to achieve the optimum balance between generating solutions that are: - crude but effective in most cases (but which the controller may reject) and - more refined solutions (e.g. taking account of weather conditions, checking further ahead for subsequent problems) but requiring more sophisticated algorithms and inputs, and hence being more costly to develop and possibly less robust. Tune detection thresholds to optimise balance between missed genuine alerts and spurious ones. Training in set order of actions for responding to alerts, including emphasis on the importance of ensuring system is updated (failure to detect may be due to out of date system information)	Reliability and integrity must be of a very high standard. Conflicts that are not detected by MTCD should be very rare. The system should check whether the tool is working (at all/ correctly). There could be inbuilt system diagnostics for failure/ corruption/missing data etc , or maybe procedures by which controllers can check regularly
		D	Delay in detection. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Spurious indication of non-existent conflict/NC This may apply to single or multiple problems, or to the special case of conflict/NC that has been resolved but is still showing	U	Controller wastes time understanding what is happening and/or takes unnecessary action on aircraft - distraction for both controller and flight crew	4		Develop appropriate 'intelligence' of detection algorithms, with tuning to local operational context and needs . Further research is required to achieve the optimum balance between generating solutions that are: - crude but effective in most cases (but which the controller may reject) and - more refined solutions (e.g. taking account of weather conditions, checking further ahead for subsequent problems) but requiring more sophisticated algorithms and inputs, and hence being more costly to develop and possibly less robust. Tune detection thresholds to optimise balance between missed genuine alerts and spurious ones. Training in set order of actions for responding to alerts, including emphasis on the importance of ensuring system is updated (spurious indication may be due to out of date system information) Training and transition process must build an appropriate degree of trust in the tool.	Integrity must be of a very high standard. The system should check whether the tool is working (at all/ correctly). There could be inbuilt system diagnostics for failure/ corruption, missing data etc or maybe procedures by which controllers can check regularly.
		D	Delay / distraction. Trust in tool is brought into question.	5		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	System prioritization of conflicts/ NCs is misleading (wrong)	U	Controller acts on conflicts/ NCs in an ineffective order	4			High intelligence and integrity of rules for alert prioritisation
		D	Delay / distraction. Trust in tool is brought into question.	5		Train controllers to 'calibrate' their responses to imperfections. Working methods should take into account the limitations of the tools	
	Clutter - too many conflicts/NCs or too much info on each conflict/ NC		Controller may become overloaded and miss some problems	3		Apply general principles of good HMI development - see HF Guidelines for further advice	Consider whether to allow individual controllers to adjust alert thresholds to reduce display clutter and if so over what range
Controller notices and responds to alert	**Controller does not notice conflict/ NC alert** *or* **Controller does not monitor concerned aircraft**		Resolution delayed.	3		Apply general principles of good HMI development for attention-getting, clutter etc - see HF Guidelines for further advice Training in changes in controller roles when supported by FASTI - see CTA for details. There may be changes in, for example, the allocation of work between and communicvations between them. Also, the nature of situation awareness may change - from picturing each aircraft to picturing conflict pairs highlighted by MTCD.	Alert the controller if any conflicts are not visible on the display (e.g. if using a zoomed-in view, or filtering of certain traffic) Require a response from the controller to acknowledge the alerts and messages. Where appropriate, an alert could be given if no response is received within a certain time.

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Controller wrongly ignores an alert (sees it as of low significance) For example controllers may currently be more inclined to look for conflicts than FL deviations, as latter can be difficult to detect. They may persist with this strategy and so not place much importance on MONA warnings, and hence not obtain the benefit		Resolution delayed.	3		Take account of different controller styles when tuning alerts - e.g. proactive controller needing later alerts as a 'safety net' warning to recover or reactive controller needing earlier alerts to prompt required action. Consult controllers on strategies they use to spot deviations - tune MONA thresholds, timings and warnings accordingly.	
	Controller does not verify problem with concerned aircraft		Controller may take unnecessary action - distraction for both controller and flight crew	4		Consider whether or not the should be a Procedure for controllers to verify all alerts with pilot. If this results in excessive (unsafe) workload it may negate the overall benefits of FASTI. A certain number of spurious alerts is inevitable, as MONA/ MTCD are predictive. The balance between spurious and missed genuine alerts should be optimised (as under the 'spurious indication' failure) by tuning the algorithms and thresholds carefully rather than relying on a remedial procedure.	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Controller misinterprets alert information (eg confuses objects selected, misreads numbers…)		Controller handles the problem in an inappropriate way.	3		Apply general principles of good HMI development - see HF Guidelines for detail	Alerts/ 'interlocks' for incorrect responses or attempts to use a function inappropriately (where detectable)
	Controller forgets or loses awareness of mode/ settings (eg thinks a lower threshold is in use, or that lookahead is further than it is)		Delay in detection.	3		Develop procedure to convey user-definable settings to next shift controller at handover (or reset them?)	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
Facilitate identification of resolutions by presenting the conflict/NC to the controller (eg by displaying it on main display/ PPD/ VAW)	**Displays wrong information about a conflict/ NC** - eg shows minimum distance as 3NM when in reality it will be 1 NM *or* **Displays a wrong conflict/NC type (e.g. wrong conflict geometry shown on main display, level bust rather than track deviation)** ***or*** **MTCD Shows only one conflict for an a/c when actually there are two or more** (failure to correlate conflicts)	U	Controller handles the problem in an inappropriate way.	3			High integrity of calculation and display of conflict information
		D	Delay in resolution. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	as above

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
Test whether a proposed resolution is conflict-free - 'What-if' probing. This includes identifying aircraft constraining the resolution of a conflict or occupying a flight level requested by another aircraft (is this latter part of conflict detsction? - i.e showing a potential future conflict if the reguest is granted) rather than to do with resolutions?	**What-if probing provides misleading information regarding the edited trajectory - eg shows proposed resolution to be conflict-free when it is not (**e.g. due to failure to identify aircraft constraining the resolution)	U	Controller handles the problem in an inappropriate way.	3			High integrity of calculation and display of what-if information
		D	Delay in resolution. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	
	Spurious constraint on resolution identified	U	Controller handles the problem in an inffective way.	4			High integrity of calculation and display of what-if information
		D	Slight delay in resolution. Trust in tool is brought into question.	5		Train controllers to 'calibrate' their responses to imperfections in MTCD. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
Transfer conflicts to TC for resolution	**PC transfers conflicts/ NCs to TC at inappropriate time** ***or*** **PC sets inappropriate thresholds for automatic transfer to TC.**		If transfer is too early TC may take actions unnecessarily or inefficiently. If too late, TC has insufficient time to respond	3		Establish adequate and appropriate ranges of detection time/ distance/ deviation thresholds, and limits on these thresholds, taking account of delivery, readback and manoeuvre time. Training in PC/TC interaction - mutual understanding of when transfers should occur	
	Automatic transfer of conflicts/NCs to TC is too early (i.e. before the threshold established by the PC)	U	TC takes actions unnecessarily or inefficiently.	4			High integrity and reliability of algorithms for transfer
		D	Slight increase in workload. Trust in tool brought into question.	5		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	
	Automatic transfer of conflicts to TC is too late, or not at all	U	TC has insufficient time to respond	3			High integrity and reliability of algorithms for transfer
		D	TC has insufficient time to respond	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
Present reminders to controller (e.g. to turn aircraft, to transfer to next sector)	**Reminder presented too early/ too late** *or* **Reminder content incorrect** (eg 'Turn HDG 230' rather than 'Turn HDG 270')	U	Controller gives inappropriate instruction (wrong time, wrong aircraft, wrong parameters …)	3			High integrity and reliability of algorithms for reminders
		D	Delay in resolution. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	
Update system after taking action in response to alerts	**Controller does not update system, or enters incorrect information**		Mismatch between instructions given to a/c and update to system - future conflict/ NC detection will be invalidated .	3		Apply general principles of good HMI development to to give appropriate cues / reminders and facilitate correct data entry. See HF Guidelines for further advice. Training in set order of actions for responding to alerts, including emphasis on the importance of ensuring system is updated (correctly)	
	Tool does not update trajectories correctly	U	Delay in or ineffective resolution.	3			Very high reliability and integrity of trajectory updates
		D	Delay in resolution. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
Facilitate screen-to-screen co-ordination and transfer between centres or sectors	**Loss or corruption of co-ordination/ transfer information, or information addressed to wrong sector (**includes message set not same for inter-sector and inter-centre co-ord)	U	Delay in or ineffective co-ord and transfer	3			High integrity and reliability of data links and displays
		D	Delay in co-ord and transfer. Trust in tool is brought into question.	4		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	
	Controller sending message makes error in entering data or addressing the message	U	Delay in or ineffective co-ord and transfer	3		Apply general principles of good HMI development to facilitate correct entry - see HF Guidelines for further advice	Provide diagnostics and error messages where possible for some more obvious errors - e.g. time given other than in a possible hh:mm format, Flight Level above or below airspace limits
	Incoming coordination/ transfer messages not noticed		Delay in co-ord and transfer	4		Apply general principles of good HMI development for attention-getting, clutter etc - see HF Guidelines for further advice	Telephone available as fall-back

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Controller overloaded with co-ord/ transfer messages. Several communication lines could be open at the same time. The messages will not in themselves convey the sense of urgency/ priority that can be given in telephone conversation		Controller does not respond to some messages and/ or makes errors in responding	3		Develop HMI to present and allow management of message queue effectively Consider limiting number of messages that can be displayed (e.g. by buffering incoming messages and showing a 'message waiting' icon, or impose 'flow control' on senders? Train controllers to decide when it is more efficient to use telephone co-ordination - e.g. for complex multiple changes or changes that depend on factors affecting the other sector and that may therefore require more discussion	Telephone available as fall-back
	Co-ord/transfer requests not answered in time or message and response misordered. Note that nessages may be sent simultaeously or cross in transit -		Controllers may become confused, miss some messages and make errors in responding to others	3		Develop HMI to present and allow management of message queue effectively	Telephone available as fall-back

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
GENERAL - applicable to all functions	**Loss of all or some FASTI functions**	U	If controller does not detect failure, conflicts and NCs may not be realised until too late	2	It would be useful to simulate some external and./or internal failures in the planned simulations, although this will be constrained by the limits on what can be realistically simulated and responded to	Training in set order of actions for responding to alerts, including emphasis on the importance of ensuring system is updated (in this case, such that system information is as recent as possible when a failure occurs (But this no difft from today?). Consider what rules are required for degraded operation - eg can MTCD be used if MONA is not available Assign clear procedures and responsibilities for deciding to reduce traffic or take other contingency actions if FASTI or component tools fail -and depending on whjat other tools/ systems renaion vailable. This is a complex issue in ATM automation, and each ANSP will need to address it in more detail, taking account of their specific context and regulations.	Very high reliability of system (eg using separate, redundant software algorithms System self-diagnostics and error messages

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
		D	Workload increase - controllers must scan for conflicts and NCs.	3		Initial and refresher training in simulations to ensure controllers can revert to working without FASTI tools.	
	Incorrect or inaccurate information provided by tools	U	Inappropriate or delayed responses	2	It would be useful to simulate some external and/or internal failures in the planned simulations, although this will be constrained by the limits on what can be realistically simulated and responded to		Very high integrity and reliability of system. System self-diagnostics and error messages
		D	Delayed or inappropriate responses	3		Train controllers to 'calibrate' their responses to imperfections. Working methods should take account of the limitations of the tool	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Over-reliance on tools		De-skilling, insufficient human monitoring, inability to revert in event of failure. Specific examples could include: - TC/PC waiting for MTCD/MONA alerts as triggers for action, or waiting for an alert even when a problem has already been noticed and could be resolved - TC insufficient checking of conflicts passed on by PC - PC spending too much time probing with 'what-if' tool rather than taking action	3		Design implementation and transition processes to develop an appropriate degree of trust . For example, consider how best to introduce FASTI - over what period and over what geographic area? Is it better to allow controllers time to build trust gradually, or is it confusing to keep introducing changes bit by bit? (This and other issues will be discussed in the Guidance, drawing on the HF Guidelines, the EEC Safe Transition report and? the SHAPE project)	

Function (broadly allocated to tools or controller where appropriate)	**Failure**	**Detected or undetected [D/U]**, where appropriate (2)	**Hazard**	**Severity ranking**	**Issues for EUROCONTROL**	**Guidance for the ANSPs**	**Safety Requirements**
	Under-reliance on tools		Over-checking of the tool outputs, such that benefits of FASTI are not obtained	4			