EUROCONTROL

SAFETY & REGULATIONS

Completing the FASTI Safety Case:
Guidance for Service Providers

FASTI

Making change in En-Route Air Traffic control

DELIVERABLE

EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Completing the FASTI Safety Case: Guidance for Service Providers

Edition Number	:	1.0
Edition Date	:	11 November 2008
Status	:	Released Issue
Intended for	:	FASTI Project Team

DOCUMENT CHARACTERISTICS

TITLE

Completing the FASTI Safety Case: Guidance for Service Providers

	EATMP Infocentre Reference:	
Document Identifier	**Edition Number:**	1.0
	Edition Date:	11/11/08

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 their tasks of conflict detection, planning, monitoring and co-ordination. EUROCONTROL's role is to co-ordinate, harmonise and expedite the uptake of the FASTI system. ANSPs, supported by industry, will be responsible for implementing operational systems. EUROCONTROL has developed a Preliminary Safety Case (PSC) comprising an argument and evidence that the concept and high-level design of FASTI (so far as these have been proposed by EUROCONTROL) could be safely put into operation. Each ANSP will need to undertake more detailed definition and design, taking account of their specific operational context and needs, and them carry out implementation, transition and operation. 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. This document contains guidance to assist ANSPs in adapting and extending the PSC to produce a full Safety Case for their own implementations of FASTI.

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	□	Stakeholders	□	Extranet	□
Proposed Issue	□	Restricted Audience	☑	Internet (www.eurocontrol.int)	□
Released Issue	☑	*Printed & electronic copies of the document can be obtained from*			

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 authors: David Nicholls - RM Consultants Ltd (Consultant Team Project Manager) Toni Close	11/11/08
EUROCONTROL Project Manager	Predrag Terzioski	11/11/08

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		Preliminary Draft (incomplete)	All
0.2	15/07/08		Draft, written to align with v1.0 of the FASTI PSC	All
1.0	11/11/08		Issued version with minor clarifications and presentational improvements	All

CONTENTS

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 and wider stakeholders, 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.

EUROCONTROL has developed a Preliminary Safety Case (PSC) comprising an argument and evidence that the concept and high-level design of FASTI (so far as these have been proposed by EUROCONTROL) could be safely put into operation. 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. These outstanding issues are currently being addressed by EUROCONTROL

The next stage will be for each ANSP to undertake more detailed definition and design of the FASTI system, taking account of their specific operational context and needs, and to plan for and then carry out implementation, transition and operation. 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.

This document contains guidance to assist ANSPs in this process of adapting and extending the PSC in order to produce a full Safety Case for their own implementations of FASTI.

MAPPING THIS GUIDANCE TO THE PRELIMINARY SAFETY CASE

This table shows where each Argument is explained in the FASTI Preliminary Safety Case (PSC), and where Guidance on completing it can be found in the present document.

Even where no specific guidance is provided, ANSPs still need to review each argument in the light of their specific operational context, needs and plans for FASTI, and taking account of their own Safety Management System.

Argument No	Argument	Relevant section / page numbers in this Guidance document	Relevant section/ page numbers in PSC
1	**Safety of FASTI Definition**	p20-31	p20-52
1.1	Intrinsic Safety of the Concept	p20-22	p20-25
1.1.1	The overall safety aims have been identified		p21
1.1.2	A Functional Model has been developed that completely and correctly interprets the Concept of Operations		p22
1.1.3	The functional differences from existing operations have been fully described and understood	p20-21	p22
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		p22-23
1.1.5	The FASTI concept has the potential to satisfy the safety criteria for the overall ATM system		p23
1.1.5.1	The FASTI concept will satisfy criterion Cr01		p23-24
1.1.5.2	The FASTI concept will satisfy criterion Cr02	p21	p24
1.1.6	The key functionality and performance parameters that affect safety have been defined and are compatible with the Safety Criteria	p21-22	p24-25
1.2	The FASTI high-level design is complete	p22-24	p25-35
1.2.1	The high-level design and its rationale are fully documented		p26
1.2.1.1	The boundaries of the system are clearly defined	p22	p27
1.2.1.2	Differences from the baseline have been identified		p27
1.2.1.3	The Logical Model is complete		p27-28
1.2.1.4	Changes in working practices and controller cognitive activities have been identified		p28-29

Argument No	Argument	Relevant section / page numbers in this Guidance document	Relevant section/ page numbers in PSC
1.2.1.5	How FASTI is to be used - the relationship between human and automation - has been fully described	p22-23	p29-30
1.2.2	The high-level design includes everything necessary to achieve a safe implementation of the concept	p23-24	p30-34
1.2.3	Dependencies on and assumptions about the external systems with which FASTI interfaces have been identified		p34
1.3	The FASTI high-level design is coherent and correct	p24-26	p35-42
1.3.1	All reasonably foreseeable normal operational conditions and range of inputs from adjacent systems have been identified	p24-25	p36
1.3.2	The high-level design is internally coherent	p25	p37
1.3.3	The high-level design functions correctly under all reasonably foreseeable normal operational conditions	p25-26	p38-41
1.4	The FASTI high-level design is robust against external abnormalities	p27-28	p42-46
1.4.1	Abnormalities in external systems have been identified	p27	p42
1.4.2	The system can react safely to all reasonably foreseeable abnormalities in external systems	p27-28	p43-46
1.5	Risk from internal failures is sufficiently reduced	p28-29	p46-50
1.5.1	Failures within FASTI have been comprehensively identified		p46
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		p47
1.5.2.1	Safety Requirements have been defined for prevention of internal failure		p47-48
1.5.2.2	Safety Requirements have been defined to mitigate the effects of internal failure		p49
1.5.2.3	Safety Requirements have been defined for fallback in the event that FASTI fails completely		p50
1.6	Suitability and sufficiency of the safety assessment	p29	p50-51
1.7	All Safety Requirements are realistic and demonstrable	p30-31	p51-52

Argument No	Argument	Relevant section / page numbers in this Guidance document	Relevant section/ page numbers in PSC
2	**Safety of FASTI Implementation**	p32-34	p52-54
2.1	All Safety Requirements identified in the Definition have been incorporated in the detailed design	p32-33	p53
2.2	Nothing in the process of implementation has introduced additional risks	p33-34	p53
2.3	Selection of the various possible physical implementation options has been carried out with sufficient regard to safety	p34	p54
2.4	Procurement has been carried out with sufficient regard to safety		p54
2.5	Detailed design has been carried out with sufficient regard to safety		p54
2.6	Construction/ integration has been carried out with sufficient regard to safety		p54
2.7	Commissioning has been carried out with sufficient regard to safety		p54
3	**Safety of FASTI Transition**	p35-39	p55-57
3.1	The existing system has been safely brought up to the baseline	p35	p55
3.2	Pre-operational validation has been carried out	p36	p55
3.3	Nothing in the Transition process has introduced additional risk	p36	p55
3.4	Safety-related training has been achieved	p36-37	p55-56
3.5	Working methods are safe and appropriate	p37-38	p56
3.6	Procedures and other required documents and resources are readily available to users and stakeholders	p38	p56
3.7	Shadow-mode operations have established safety in a realistic operational context	p38	p56
3.8	Pre-FASTI systems has been safely removed (or left in place as fallback	p38	p56
3.9	O-date itself and initial operations safely carried out.	p39	p57
4	**Safety of FASTI Operation**	p40-42	p57-58
4.1	Post O-date monitoring and feedback continue to ensure safety in operation	p40-41	p57
4.2	Maintenance and upgrades/ updates are safely performed	p41	p57
4.3	Changes in the operational environment are identified and responded to	p41	p57
4.4	FASTI is safely decommissioned at the end of its life	p41-42	p58

1. INTRODUCTION

This document contains guidance to assist ANSPs in developing a Safety Case for their operational implementation of FASTI.

1.1 The FASTI Programme

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.

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

FASTI should result in a shift from sector-focussed, tactical and reactive traffic management to a more trajectory-oriented, strategically-planned, conflict-free approach.

EUROCONTROL's role is to define a concept and high-level design for FASTI and to co-ordinate, harmonise and expedite the uptake of the FASTI system by ANSPs. ANSPs, supported by industry, will be responsible for implementing operational systems.

1.2 The FASTI system

A description of the FASTI system is provided in the PSC. Only the key points are summarised here.

The key features of the FASTI Concept of Operations as developed by EUROCONTROL [Ref. 5] are that the controller will have new automated tools available to support monitoring for non-conformances and conflicts, and related actions, and to support co-ordination between controllers. This should free up controllers' cognitive resources, by automating and/or supporting some of the more routine activities that currently account for a lot of controllers' workload.

The tools currently included in the FASTI Programme are described below. It is stressed that the Safety Case must consider all elements of the FASTI system, i.e. the People, Procedures and Equipment (hardware and software) associated with these new automated tools.

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; and
- 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.

1.3 The Safety Case process

In order to comply with EUROCONTROL policies and meet the wider safety aspirations of the aviation community and its stakeholders, it is necessary to carry out a thorough and systematic safety assessment before making any significant changes to ATM systems. In particular, the safety of any significant new system (such as 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. The Safety Case provides the ANSP itself with an assurance of safety, and should also serve as a basis for licensing and auditing by national safety regulators.

EUROCONTROL has developed a Preliminary Safety Case (PSC) [Ref 1] comprising an argument and evidence that the concept and high-level design of FASTI, so far as these have been proposed by EUROCONTROL, could be safely put into operation. The PSC also outlines possible argument structures for later stages in the lifecycle.

A number of points (Safety Issues) remain to be addressed before EUROCONTROL's PSC can be finalised. The main needs are to ensure that adequate ANSP input is obtained, and that appropriate simulations are carried out. These outstanding issues are currently being addressed by EUROCONTROL.

EUROCONTROL cannot provide evidence to argue the safety of any particular operational FASTI system, as this will be a matter for the ANSPs. Each ANSP will need to undertake more detailed definition and design, taking account of their specific operational context and needs. They will then need to plan for and carry out implementation, transition and operation. In parallel with these practical stages in the lifecycle, ANSPs will need to adapt and extend the PSC into a full Safety Case, which will ultimately cover the operational system. This Guidance document is intended to help ANSPs with that process.

2. HOW TO USE THIS GUIDANCE

2.1 Who is it for?

This Guidance is written principally for use by ANSP staff who are responsible for assuring the safety of new projects and, in particular, those responsible for developing the Safety Case.

In developing the Safety Case you will need to draw on various areas of specialist expertise: ATM operations, human factors, software development, system integration and so on. It is not necessary to be a specialist in these areas, only to be able to understand enough about each specialist area to be able to bring them together to produce a coherent safety argument for a safe system. The PSC and the Guidance are structured to help you with that process by providing a top-down view, which will help you to develop a complete and coherent Safety Case.

The Guidance may also be of use to regulators. By setting out a general framework for a Safety Case, not weighed down with technical detail of any specific system, it may help the regulators to identify key points and priorities for audit or detailed scrutiny when reviewing operators' Safety Cases.

2.2 Scope of the Guidance

EUROCONTROL has published generic guidance on Safety Cases and safety assessment [e.g. SCDM [Ref 2] and SAM [Ref 3]]: that guidance has not been repeated here. Rather, assuming a reasonable familiarity and understanding of the generic principles, the emphasis is on demonstrating how they can be put into practice for FASTI.

The Guidance does not provide advice on the technicalities of design, implementation, and operation, such as software development, system architecture and integration, procedure development and controller training. ANSPs and/ or their suppliers are expected to have the necessary expertise in these areas; the Safety Case provides a framework for ensuring and demonstrating that these specialist disciplines work together to achieve a safe system.

It is essential that implementation, transition and operation are conducted under a suitable Safety Management System. This Guidance document covers the specifics of FASTI, not general considerations of ATM safety management.

2.3 Steps in the Process and Structure of the Guidance

The Guidance is structured around the Safety Argument in the PSC, which reflects, broadly, the stages in the lifecycle. Table 1 shows the main steps you will need to take in order to build your own Safety Case, relating these steps to the high-level Arguments and lifecycle stages.

Many ANSPs already have their own way of dividing up the lifecycle and Safety Case stages, defining milestones and review/ sign-off points. You do not have to align the details of your formal safety management process with that shown in Table 1, but you should ensure that all the steps are covered in some way – you could use this table as a high-level checklist.

Table 1 Steps in developing your Safety Case

Step	Lifecycle Stage	Description	Relevant Section of Guidance
Clarify your vision for FASTI	Definition	Every ANSP is different and will implement FASTI in different ways. You will need to make a number of key decisions about what you what to achieve with FASTI, and these will affect the way that you build your Safety Case.	Section 3
Review / adapt/ develop the overall Safety Argument	All	You will need to review the overall safety Argument and adapt/ develop it where necessary. However, as the argument structure is designed to be applicable to most ATM systems, it is not expected that much change will be necessary at this level.	Section 4
Review / adapt/ develop Argument 1	Definition	You will need to review Argument 1 and adapt/ develop it where necessary. As EUROCONTROL's definition of FASTI is intended to be suitable for any en-route ECAC centre, you will probably not need to change the structure or high-level content of this Argument very much; it has been quite fully developed already in the PSC. However you will need to add detail.	Section 5
Develop Args 2, 3 and 4	Implementation (Arg 2) Transition (Arg 3) Operation (Arg 4)	These stages lie largely outside EUROCONTROL's remit: the arguments are only developed in outline in the PSC for Arg 1. You will therefore need to do a more substantial amount of new work to structure these arguments and complete the evidence.	Sections 6, 7, 8

Within each step, the Guidance indicates the Arguments that you are most likely to need to adapt or extend. For each such Argument, we provide assistance in completing it, under 'What/ How/ When/ Who' headings, like this:

What?

When?

How?

Who?

The ‘What’ is always described, but we cannot always give much, or indeed any detail of ‘How’, ‘When’ or ‘Who’, since these will depend on ANSP-specific factors such as your time schedule, organisational structure and skills available.

The table at the front of this document maps the content of this Guidance to that of the PSC document, showing where each Argument is explained in the PSC and where Guidance on completing it can be found in the present document.

2.4 Using your Safety Case

Although it is important to have produced the final Safety Case document, you should always keep in mind the fact that the process of completing the Safety Case is as important as the finished product:

- The activities you will undertake should be well planned and anticipated; however, there will be lessons learnt during this process that can be fed back into the design and will improve the final system.
- The process will serve to introduce the new system to its users, and help to encourage involvement and buy-in.
- Many regulators will be more receptive to the safety claims of an organisation demonstrating sound development methodology, than to one who produces many pages of test results.

The process of developing a Safety Case should be seen as part of your organisation’s commitment to safety and quality management.

2.5 Building on the PSC

EUROCONTROL aims to encourage harmonised approaches to safety and avoid duplication of effort. You should make the best use of the work already undertaken in the PSC, but it is not enough simply to ‘cut and paste’ sections of the PSC. You need to review all aspects of the PSC thoroughly and correctly adapt and extend it where necessary. Even where no specific guidance is provided in this document, review the Arguments in the light of your specific operational context, needs and plans for FASTI, and taking account of your own Safety Management System.

You cannot assume that the PSC or Guidance will alert you to every safety consideration; issues may arise that cannot be foreseen at this stage. You therefore need to ensure that you consider your own system in an independent, open-ended way.

For example, the Safety Argument approach has a danger of encouraging ‘confirmation bias’ – i.e. seeking only the evidence that supports what you would like to prove. A more scientifically justifiable approach would be to think in terms of trying to falsify the hypothesis that FASTI is safe. You should take a challenging approach to the Safety Argument. It is advisable for ANSPs to have their own peer reviewers (rather than leaving this function to the regulator) who can challenge what is presented and look in an open-ended way for contrary evidence.

3. CLARIFYING YOUR VISION FOR FASTI

What?

Before getting into the safety arguments and evidence themselves, it is important to understand where you are now, decide what you want to achieve with FASTI, and how you will implement and use it to realise these aims. These factors and decisions will define what is special about your intended implementation, and hence provide the high level context for reviewing what is already in the PSC, and building your own Safety Case.

They will also affect your more detailed work on the Arguments and Evidence. The areas where changes are most likely to be needed are flagged up for you in Sections 5 to 8 although – as noted in Section 2.5 - this may not be comprehensive.

How?

We suggest that you document your vision for FASTI in an introductory part of your Safety Case. At this point, detail is not required, just a paragraph or two should be sufficient to outline each of the main factors and decisions. Clarifying the vision is part of developing your Concept of Operations, and your 'ConOps' document is likely to contain more detail. Later, more detailed Arguments will all need to be reviewed in the light of how your evolving Concept of Operations differs from, or adds more detail to, EUROCONTROL's 'typical' Concept of Operations. The development of the Concept of Operations will of course be iterative with the Safety Case, but a clear and reasonably stable vision is essential as a starting point.

As well as documenting what decisions you have made, it is important to record why you have made them. This will help to avoid the danger of future users changing the system without understanding why it is as it is.

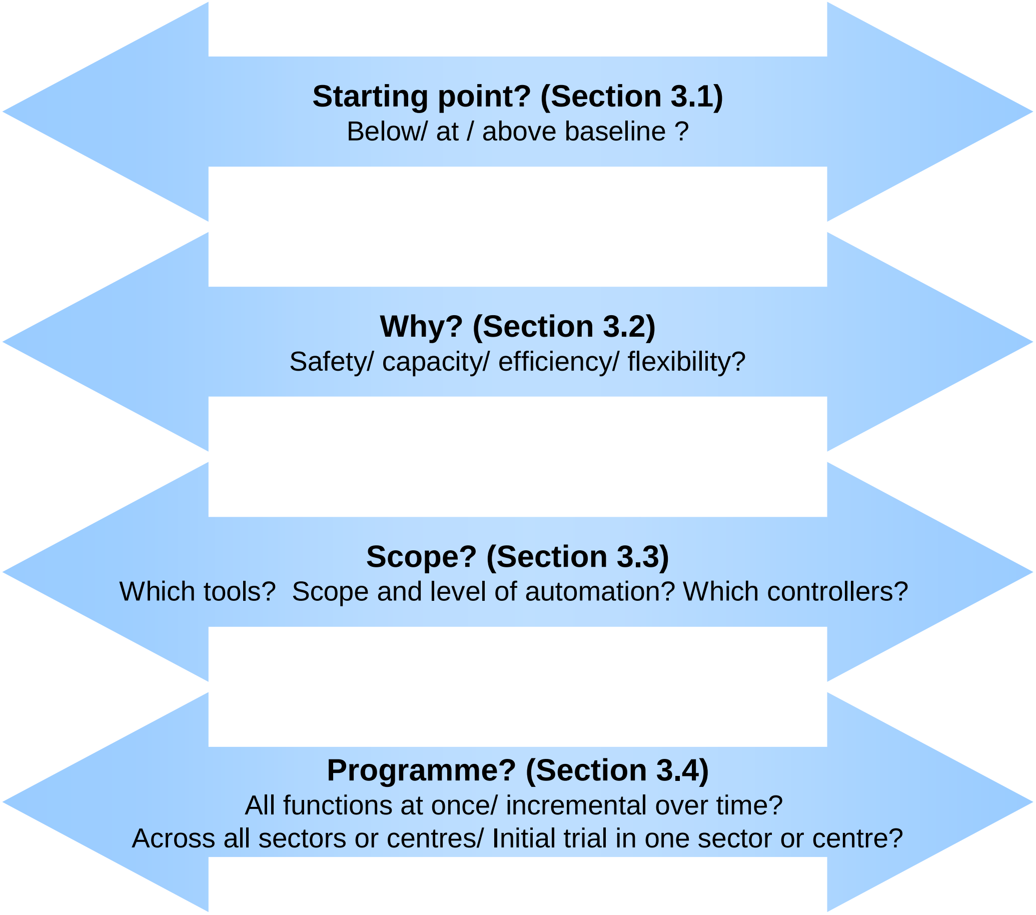
When?

You will need to make these decisions as early as possible in the process. You will then be able to establish a plan, including cost, resourcing and timescale, for getting to an operational FASTI system and the associated safety activities.

Who?

It is important that you involve stakeholders in these high-level decisions as far as possible: the project management team, the controllers, the designers and suppliers, etc. Some decisions may also depend on whether your neighbours are implementing FASTI, so get them involved too. It is essential that there is a common vision of what FASTI involves and what it is for.

An overview of the key factors and decisions (which may be inter-related) is given in Figure 1. They are described in more detail in Sections 3.1 to 3.4.



Starting point? (Section 3.1)
Below/ at / above baseline ?

Why? (Section 3.2)
Safety/ capacity/ efficiency/ flexibility?

Scope? (Section 3.3)
Which tools? Scope and level of automation? Which controllers?

Programme? (Section 3.4)
All functions at once/ incremental over time?
Across all sectors or centres/ Initial trial in one sector or centre?

Figure 1. Your vision for FASTI - key factors and decisions

3.1 What is the starting point?

The questions you will need to answer are:

1. *What is your baseline, and how does it differ from that assumed by EUROCONTROL?*

Each ANSP will begin to implement FASTI from a different starting point. EUROCONTROL has assumed a baseline (see Appendix C of the PSC) that is intended to be typical of common European systems, but it is nevertheless hypothetical, and real baselines may be different. Compare your baseline with the assumed one. Do you need to add anything to your system before you can implement the FASTI tools? Or do you already have some elements of FASTI in place?

2. *How do you intend to deal with these differences in the Safety Case?*

   If you need to implement some enabling measures to bring your current system up to the baseline, you must provide assurance of the safety of these enablers as well as of the changes from baseline to FASTI. This could be done in a separate Safety Case for the enablers or in an integrated Safety Case covering both the enablers and FASTI. The choice will depend on the phasing of the changes (will the enablers be put into operation well before FASTI or just in time?) and the degree of technical and project management overlap (will the same team be involved in the enablers and FASTI, or are they separate projects?).

   If, on the other hand, you already have some FASTI tools or similar tools in operation, and you have a sound Safety Case for them, you should be able to make faster progress by integrating it with the Safety Case for the new FASTI elements.

3.2 Why implement FASTI?

ANSPs will have varying reasons for implementing FASTI. Some may wish to take all the benefits of FASTI in terms of safety improvement, while others will want to trade some or all of this benefit[1] for gains in capacity, or operational flexibility and efficiency.

You need to have a clear idea of why you want to implement FASTI and to have a coherent rationale for that. If you are looking for a mixture of benefits, what is the relative priority for each?

Eventually, you should be able to justify your reasons and agree them with your national safety regulator, with due regard to wider European and international aims.

[1] There is often a trade-off between safety and capacity, flexibility or efficiency. But this is not always the case – in the detailed design and implementation you should be looking for 'win-win' cases. For example, a design that allows greater flexibility can also be safer, because it allows the controller more freedom to choose the safest option. FASTI may have a positive financial effect as well as a safety benefit – it is not necessarily a matter of trading safety benefit against cost.

The questions you will need to answer are:

1. *Can the current risk be considered tolerable?*

   If not, safety must be improved, and FASTI can be one way to do this.

2. *What are the stakeholder demands and internal business plans with regard to safety, capacity, flexibility and efficiency?*

   A key parameter affecting where you set the balance between these benefits is the traffic density in the airspace [Ref. 23], as outlined below:

   - In low density environments, where workload reduction is not a priority, FASTI could be used to provide a safety backup and hence allow single manning of sectors or an increase in the area covered per controller, giving an increase in efficiency. These benefits also apply to higher traffic regions at night and at other times when the traffic level is predictably low.
   - Medium density: As traffic density (and complexity) increase, automation offers more stable traffic flows and a workload reduction to the controller, enabling an increase in capacity. FASTI is also an enabler for introducing common procedures that will increase the ability of controllers to operate different airspace regions. (If airspace is made more dynamic, as is planned in other European programmes, geographic sectors will become less relevant and controllers will need to become less specific to a particular region.) FASTI may also enable improved utilisation of airspace through the Multi-Sector Planner (MSP) concept, although there is only limited experience of this to date.
   - High-density: The major benefits offered to high traffic regions come from the stabilisation of the traffic flows, ‘designing-out’ conflicts. Maximising the detection and resolution of conflicts/ non-conformances at the planning stage reduces controller workload.

3. *Can any increases in capacity be justified in relation to transport and environmental policies?*

4. *What other developments are occurring that may change the balance of benefits you expect from FASTI?*

   For example, if you have another project ongoing that will deliver a substantial increase in capacity, then you might want to use FASTI as one of the ways to maintain safety, rather than to add to capacity in its own right.

3.3 What is the scope of FASTI?

FASTI has been defined such that it could, in principle, be implemented in any en-route ECAC airspace where traffic is under radar control. However, every ANSP and centre has special features and challenges that distinguish it from its neighbours and ANSPs will, as noted in Section 3.2 above, vary in their reasons for implementing FASTI. You will therefore need to adapt the scope of FASTI to match these factors.

The questions you will need to answer are:

1. *Which tools do you want to implement?*

   The FASTI programme considers all three tools, MTCD, MONA and SYSCO as a package, but some ANSPs may wish to implement only some.

2. *What scope and level of automation do you want?*

   The general principles for responsibility sharing between controller and automation are set out in EUROCONTROL's Definition, but within these general principles FASTI can be implemented with different scopes and levels of automation. This will need to be considered in greater detail in your development of Arg 1.2.1.5, but at this stage you should consider your automation strategy in broad terms. In the simplest terms, if future demand is likely to exceed the controllers' workload capacity, automated support will be needed. But your decision must also take into consideration the implications of automation on training requirements, recruitment, supervision, and job satisfaction.

3. *Which controllers will use the FASTI tools?*

   Some ANSPs may intend MTCD, for example, to be a tool for the PC only, while others may want to make it available for the TC as well.

3.4 What is your programme?

The way in which FASTI is rolled out for operational use can vary. You might decide to implement FASTI incrementally, making some small changes initially for a "quick win", or introducing it in just one sector first in order to build up confidence and limit project risks. Or you might decide to implement the full functionality across the whole Centre in one go.

The questions you will need to answer are:

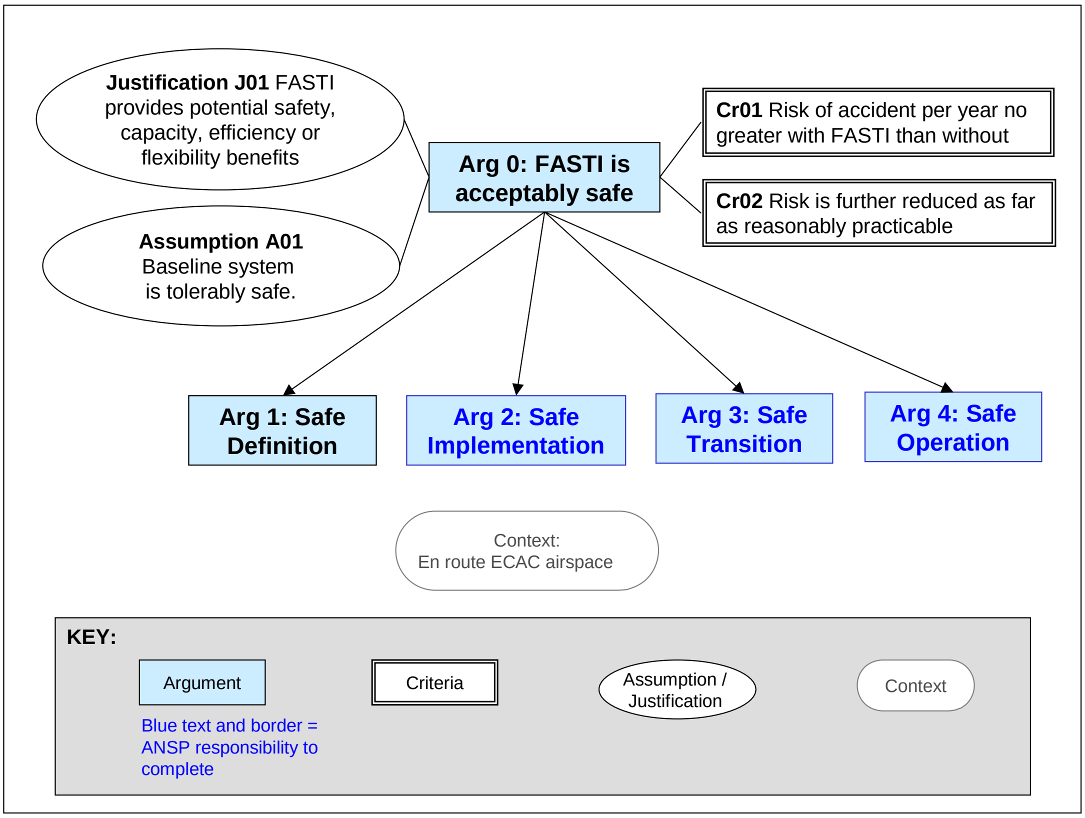
1. *What are the dependencies, both internal and external, that may constrain the implementation programme?*

2. *Will the full FASTI system be implemented all at once or will the tools and functionality be introduced in stages?*

3. *Will FASTI be implemented in all your sectors/ centres at the same time, or initially just in one trial area?*

4. REVIEWING THE OVERALL SAFETY ARGUMENT

The technical core of the PSC is a Safety Argument: a systematic, hierarchical presentation of the arguments, substantiated by evidence, supporting the top-level Claim that **the concept and high-level design will be acceptably safe for operational use.**



Justification J01 FASTI provides potential safety, capacity, efficiency or flexibility benefits
Assumption A01 Baseline system is tolerably safe.
Arg 0: FASTI is acceptably safe
Cr01 Risk of accident per year no greater with FASTI than without
Cr02 Risk is further reduced as far as reasonably practicable
Arg 1: Safe Definition
Arg 2: Safe Implementation
Arg 3: Safe Transition
Arg 4: Safe Operation
Context: En route ECAC airspace
KEY:
Argument
Criteria
Assumption / Justification
Context
Blue text and border = ANSP responsibility to complete

Figure 2. The Overall Safety Argument

At this overall level, the argument developed in the PSC is very general, being applicable to all the foreseen variations in implementations of FASTI. Indeed, very similar overall argument structures are being used by EUROCONTROL for a wide range of other ATM systems. It is therefore anticipated that ANSPs will not need to make any major changes to its structure or high level content. The completion of each of the lower level Arguments that cover each main stage in the lifecycle is detailed in Sections 5 to 8.

What?

However, it is important that you review the overall argument early on in the process and provide more specific evidence where required. In particular, you need to review the Justification, Criteria, Context and Assumptions as described in Sections 4.1 to 4.4.

When?

This review of the overall argument needs to be carried out early on in the process, as it will affect the way in which you develop the more detailed arguments

4.1 Justification

The PSC gives a justification for FASTI at the pan-European level.

What?

Make sure that this general justification for FASTI properly reflects your own broad vision for implementing FASTI: the reasons that you considered in Section 3.2. Is FASTI being implemented for safety benefit, for gains in capacity, flexibility or efficiency, or for some mixture of these? Whereas Section 3.2 states *what* your vision is, the Justification is the place to document more formally the *rationale* for your decision about the balance of benefits.

Further detail of how this vision, and the justification for it, translates into detailed safety targets can be given in your description of the criteria, as described in Section 4.2.

4.2 Criteria

Two criteria, **Cr01** and **Cr02**, have been adopted in the PSC, in line with generic EUROCONTROL safety policies.

What?

Review these criteria and amend them if necessary to ensure compatibility with any generic safety policies and criteria adopted by your national regulator or within your own organisation.

4.2.1 Cr01 - probability per year of an accident to be no greater than for baseline

What?

Define what safety metrics are used to establish satisfaction of Cr01. ANSPs may have rather different definitions of what constitutes an accident from that in ESARR4, or may extend this criterion to apply to incidents as well as accidents. Consider carefully whether the safety metrics you use are appropriate, in relation to the overall principle that overall danger (the number of 'accidents') should not increase, despite traffic growth.

How?

Because it is very difficult to predict whether an accident will actually occur, it is usual to assess the changes in risk from new systems using 'lower-level' indicators, such as rates of failures, errors and incidents, or the extent to which safety barriers are breached. You will therefore need to consider carefully what practical measures to adopt and whether they are good indicators of the accident rates that, ultimately, you want to control. For example, could the incident to accident ratio, as well as the incident rate, be changed by the introduction of FASTI?

You might need to adapt this criterion to reflect your baseline. Cr01 is defined relative to the assumed baseline (see Section 3.1) in order that safety should be tested against a consistent benchmark. Otherwise, an ANSP could claim a safety benefit for the enablers necessary to bring the current 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. However, where an ANSP has already implemented some elements of FASTI or

FASTI-like tools, such that they are ahead of the assumed baseline, it would not be acceptable to allow the implementation of the rest of FASTI to degrade safety.

4.2.2 Cr02 - risk to be further reduced as far as reasonably practicable

For Cr02 you should, as with Cr01, review your safety metrics. Do they reflect the overall principle being aimed for, and are they practical?

What?

Explain clearly what ‘as far as reasonably practicable’ means to you. States and ANSPs will differ in how they interpret this term. Your interpretation must be linked to, and compatible with, your decisions about the balance of benefits and your rationale for this, which you will have described in the Justification.

4.3 Context

The PSC considered only a very general operational context: en-route airspace in the ECAC area. To develop the full Safety Case, more detailed information about the operational context will be required at various points in the argument.

What?

You need to have a clear understanding of your own operational context, including factors such as:

- airspace: class, type (e.g. en-route or E-TMA), size and geometry of the sector(s), route structures, transit times;
- traffic density and complexity e.g. the proportions of climbing/ descending crossing aircraft; holding patterns;
- presence of military or other restricted airspace; procedures for activation/ deactivation of temporary features such as Temporary Segregated Areas (TSAs);
- people involved and their working arrangements (e.g. whether PC/ TC team, SPO or MSP, task distribution between TC and PC, shift handover procedures;
- characteristics of adjacent airspace, whether and at what level they are implementing FASTI, whether en-route, terminal, oceanic or uncontrolled; whether managed by same ANSP or same State as your airspace, whether ECAC or non-ECAC;
- aircraft performance (speeds, climb/ descent rates, turn rates), equipment fit (navigation systems ..) and air operator procedures (for both civil and military operators);
- weather – for example extremes of wind speed and other conditions that can cause problems for ATM, such as thunderstorms, or wind-related runway switches.

How?

Start with very broad descriptions initially and add detail only where it becomes necessary, as your Safety Case develops, in order to develop the argument or provide evidence. Such needs are likely to emerge in Arg 1.3.1 in particular. There is a danger otherwise of producing large amounts of data that are not actually relevant to the Safety Case, which is both inefficient and distracting.

4.4 Assumptions

The only high-level assumption in the PSC is that the typical current ATM system (the baseline) into which FASTI will be introduced is acceptably safe. This will, at least initially, be an assumption for most ANSPs rather than an Argument that can be proved with Evidence. Few if any existing systems have been subjected to comprehensive, rigorous safety assessment and consideration of what 'acceptable' actually means. Hence there is unlikely to be any formal demonstration that current risks are acceptable.

What?

Review this assumption, and such evidence as may be available to support it. Is it acceptable to live with the assumption, or is there a need for a more systematic risk assessment of the current system and more clearly-defined criteria for acceptability?

Bear in mind that this assumption is not just an assumption for FASTI – it will arise in relation to any proposed change. It is recommended that you seriously consider developing a Unit Safety Case, demonstrating acceptable safety for your ongoing operation, and providing a baseline against which any future change can be assessed. Without this, your Safety Cases will not have a solid foundation and, when several changes are made, the situation may become unmanageable [Ref 15].

You should also identify and document any other major assumptions on which your safety argument will depend.

How?

It is important to look for high-level[2] assumptions that may be overlooked, as 'too obvious'. One way to do this would be by holding a structured safety brainstorming session with a wide range of stakeholders. You could structure the session around the Safety Argument (so far as you have developed it), encouraging the participants to challenge it and ask 'what does this depend on?' questions.

[2] As you develop the Safety Case, you are likely to have to make many, more detailed, assumptions. Most of these will eventually be confirmed as the design and implementation progress. For example, you may have to assume things about the operational procedures until the procedures are actually written and tested.

5. REVIEWING THE SAFETY OF THE FASTI DEFINITION (ARG 1)

Arg 1 is concerned with the safe definition of FASTI in your own setting. The definition stage of the lifecycle comprises:

- the concept (your vision for FASTI); and
- the high-level design: how you will implement and use FASTI.

The concept and high-level design must have the potential to be acceptably safe – i.e. they must be capable of satisfying the safety criteria, as well as delivering the non-safety benefits you want, subject to subsequent safe implementation, transition and operation.

EUROCONTROL has developed Arg 1 for their ‘typical’ definition of the FASTI system. Because this definition is intended to be suitable for implementation in any en-route ECAC centre, Argument 1 as presented in the PSC is quite general, and the main activity for ANSPs is therefore to review it, adapting it only where necessary. The general process steps in this activity are therefore:

- to read, carefully and critically, the version of Arg 1 in the PSC, including its sub-arguments and evidence;
- to review Arg 1, in the light of how your specific concept and high level design differ from, or add more detail to, EUROCONTROL’s ‘typical’ one (i.e. in the light of your answers to the questions posed in Section 3); and
- to adapt or develop Arg 1 if required.

For some sub-arguments, we can already see a need for specific changes and additions by each ANSP. In the following sections we summarise each such argument and give more detailed (‘what/ who/ when’) guidance on how to apply the general process to that argument.

5.1 Arg 1.1: Intrinsic Safety of the Concept

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

This argument requires you to answer the question: ‘*what will be the differences between the way things are done today and the new FASTI system?*’. 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 shown in the PSC, 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.

What?

Because you may choose to implement only some of the three automated tools, and because the functional scope of each tool is flexible, you should review and refine this description of the differences, taking account of your choices about the scope of what is to be implemented (Section 3.4). For example, if SYSCO is not implemented, the performance of the CORT function is probably not improved.

Arg 1.1.5.2 *The FASTI concept will satisfy criterion Cr02*

Cr02 requires safety risk to be reduced AFARP. The aim of this Argument is to show that FASTI enables this criterion to be satisfied.

In the PSC, EUROCONTROL showed how the FASTI concept can be used to obtain a pure safety benefit, or to trade some of this for gains in capacity, efficiency or flexibility. Hence in the PSC we could already say that, *in principle*, the FASTI definition enables Cr02 to be satisfied; in that it allows ANSPs the ability to make their own decisions about what is reasonably practicable and how safe is safe enough. Hence there should be no need for you to change Arg 1.1.5.2 itself. Later, in Args 2, 3 and 4, you will demonstrate that the implementation, transition and operation of the system will *actually* deliver these benefits and thus satisfy Cr02.

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

This argument requires you to define the key parameters that affect the safety of FASTI, and to set threshold values that will determine whether, in practice, your implementation of FASTI is meeting the safety needs.

In the PSC, the following parameters were proposed:

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.

What?

To complete this Argument, you should define thresholds of acceptability for each of these parameters (and refine their definitions if required) in order to reflect the specific levels of safety or other benefits that you require.

How?

For example, if your intention is to increase capacity by 10%, while keeping the risk per year the same, then, in very broad terms, you should look for at least a 10% increase in parameters (a) and (b). We say ‘at least’ because not all of the improvement in detection and resolution at planning stage necessarily gets translated into capacity benefit; there are other constraints and bottlenecks in the ATM system.

Note that the key parameters are simply-described operational variables that, in principle at least, could be observed in practice, rather than more ‘technical’ parameters, such as the precision of an algorithm, or reliability of a display component. This helps stakeholders involved in discussing thresholds to envisage how they relate to safety. However, the chosen key parameters are not necessarily easy to measure or most informative in validation or operational monitoring, and other metrics are likely to be needed for these purposes, as discussed in Arguments 1.3.3 and 4.1.

Who?

Involve both operational experts and designers in the discussion in order to ensure that all the relevant factors are considered. It is unlikely that you will be able to define precise numerical targets, as this type of calculation can be very complex and uncertain, but the process of discussion will help you to understand more precisely how benefits arise and can be maximised. The outcome should be some practical aiming points for designers in the implementation stage[3].

5.2 Arg 1.2: The FASTI high-level design is complete

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

This argument requires you to answer the question: '*what is included when referring to "FASTI", and what is not?*' Because ATM is a highly interdependent system, into which FASTI will be integrated, it is not possible to draw a simple physical boundary. In the PSC, 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; and elements that will not change.

What?

Review the Logical Model and, adapt it to reflect any differences in boundaries and responsibilities due to particular organisational structures or system architectures within your Centre, or due to different airspace divisions and characteristics of neighbouring sectors.

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

In order to satisfy this Argument, you need to explain and justify your automation strategy.

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.

[3] Note that the PSC suggested that EUROCONTROL should consider whether it may be possible to define example thresholds for a typical implementation (e.g. MUAC), and hence provide a model for this process.

What?

There is flexibility within these general principles to implement FASTI with different scopes and levels of automation. You need to decide on and develop a more detailed strategy, and describe it, together with its rationale.

How?

As an example of what is meant by scope of automation, MONA may be implemented to detect a limited or more extensive range of non-conformances (e.g. area infringements as well as non-conformances in route and level).

As an example of what is meant by level of automation, the 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 threshold.

In making decisions about automation, look ahead to transition and operation issues: how will controllers be trained, how will individual differences be accommodated, and how will an appropriate level of trust be built? Controllers need to know the limits of the tools and, within those limits, trust the tools to get on with it while keeping an overall lookout for problems (higher-level monitoring).

You will need to consider carefully what you actually mean by 'responsibility'. This is likely to involve consideration (outside the scope of the safety case) of legal issues

Once the level of automation has been decided, you will need to ensure safe use of the tools by defining prescribed working methods and procedures, in particular for the task distributions between controllers and automation, and by designing appropriate affordances[4] for the tools and interaction objects on the HMI. These will be considered further in Args 2.1 and 3.5.

Who?

Operational controllers should be involved in these decisions, as well as system designers.

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

This argument is concerned with showing that the system elements, as shown in the Logical Model, contain everything necessary to implement the concept. Table 3 of the PSC lists Safety Requirements (SRs)[5] related to each such element.

What?

Review the SRs in the light of your vision for FASTI and context, and emerging design and implementation plans. With sufficient reason, documented in your Safety Case, you may decide not to implement all of the SRs, to amend them or to introduce additional ones.

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

[5] As in the SAME approach, we suggest that you do not need to make the traditional distinction between 'Operational' Requirements and Safety Requirements – virtually all Operational Requirements have some significance for safety, and the successful operation of the system is necessary for safety.

You will also need to develop these (and other) SRs to provide more detail. The list of SRs in the PSC has deliberately been kept at a high level with general descriptions. At the same time, you should develop a 'tighter' wording for SRs – aim to define them in terms that will make it as clear as possible whether or not they have been satisfied.

How?

Check the EUROCONTROL FASTI website: www.eurocontrol.int/fasti/public/subsite_homepage/homepage.html for the latest FASTI documents, as these will contain useful source material.

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

***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 normal practice. This argument aims to show that this range of conditions has been identified. It requires you to answer the questions: '*in what situations do we expect FASTI to be used, and what data might it have to deal with?*'

What?

Review the parameters listed under this Argument in the PSC in the light of your context description (Section 4.3). You may need to refine or add to the descriptions of the parameters. For each parameter, determine what range of values it may have in normal operations.

How?

For each parameter, ranges can be determined from analysis of historic data, predictive methods or simply from the experience of your operational controllers and other experts.

You will find that some of these ranges can be defined quantitatively, i.e. in terms such as:

> *'transit times across the sector range from 10 to 45 minutes'*

while others will be qualitative, e.g.:

> *'to the east, the adjacent sector AAA is planning to implement FASTI, while to the west BBB is an oceanic sector'.*

This information will be important in your detailed design (Arg 2), to ensure that FASTI can cope with the range of data inputs, and in planning simulations that will test FASTI across conditions that span the range likely to be encountered in practice.

As well as determining suitable ranges for each individual parameter, note any correlations between parameter values. For example, traffic pattern and complexity may be correlated with the activation/ deactivation of SAs, or with the weather.

The information you give in this Argument should move on a stage from the general descriptive information that you gave in the Context (Section 4.3). In Section 4.3 we were looking for a overall picture of your operational context; here the important thing is to define the ranges of specific parameters that will be used in the design[6]. However, you still

[6] There is of course no very precise boundary between these two aims, and it does not actually matter very much whether the information is in one place or the other.

need to be careful to avoid generating lots of detailed data that will not be used. You can always add more detail if necessary as you begin to use the information in the detailed design and simulation planning.

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

This argument aims to show that the FASTI system will be provided with consistent and up to date data, both within and between sectors, and that it will use these data in consistent ways. It requires you to answer the question: '*have we made sure that all the data in our system will be expressed, transferred and used in a consistent and timely way?*'

This argument has not been developed very far in the present PSC because the operational concept and design documents available at the time did not contain sufficient detail of the information flows between system elements. The Logical Model shows information flows to, from and within the FASTI system, but only at the highest level.

It has been suggested that EUROCONTROL should define these information flows at some greater level of detail and hence identify any additional Safety Requirements for internal coherence that may be required.

What?

However far EUROCONTROL decides to go in providing greater detail, there will always be some matters that depend on specific implementations – i.e. on the hardware and software at individual centres, and how the FASTI tools are integrated with existing systems. You will need to define how data in your system will be expressed, transferred and used in a consistent and timely way.

How?

One way to analyse design coherence (at a level suitable for the definition stage of simpler and less critical systems) is through structured, desk-top analysis sessions with technical 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?').

When?

These analysis sessions should be done before, and in preparation for, the simulations, as they will help ensure that the simulations cover all the important aspects that can be simulated, as well as revealing issues that cannot be simulated. The sessions might effectively be combined with other workshop-type activities – e.g. the review of Assumptions, or with early stage FHAs. In later stages of the lifecycle (Arg 2), more detailed work on design coherence will be required by, for example, your software developers and system integrators.

***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 the normal operational conditions that you 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.

The PSC presents a framework for the argument and EUROCONTROL is expected to provide some further evidence to support it. This will be a combination of:

- theoretical evidence (e.g. building on the desk-top walk-through analysis described in Arg 1.3.2 of scenarios),
- evidence collated from ANSPs who are already implementing FASTI-like tools, and
- evidence from EUROCONTROL's own simulations.

However, there will still be some implementation-specific aspects that each ANSP will need to consider. The main way in which you will satisfy this Argument is by running simulations. EUROCONTROL can carry out simulations for some typical implementations and situations, but it would not be adequate simply to append the results of such generic simulations to site acceptance testing of your own system.

What?

You will need to carry out high-fidelity, site-specific real-time simulation (RTSs) of the functionality and performance of your specific FASTI concept and design. The simulations should be dynamic as well as steady-state.

How?

The Validation Plan that EUROCONTROL will draw up for its simulations will form a useful starting point for planning your own simulations, but some key factors that you will need to review and develop include:

- The need to simulate across the range of potential parameter values, and parameter value combinations, that you identified in Arg 1.3.1. It would be impracticable to test every possible combination, but you should aim to span the ranges of possible inputs as fully as possible.
- The need to define appropriate and practical safety metrics. Some potentially suitable metrics have been suggested in Table 4 of the PSC, but you should review these, taking account of their relationship with the key safety parameters that you defined in Arg 1.1.6 (how good an indicator are they?), limits on the fidelity of your simulation (how completely and accurately does it reproduce reality?) and practical issues in measurement. This last point applies especially to attempts to measure error/ incident rates – you should consider carefully how likely it is that you will actually see any occurrences during the simulation time.

For more complex and/or more critical systems, the demonstration of the correct operation of the logical architecture may also require more sophisticated, formal system-engineering methods.

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

***Arg 1.4.1** Abnormalities in external systems have been identified*

This argument requires you to answer the question: '*what could go wrong in other systems that might affect the safety of FASTI?*'

The external systems that have specific interfaces with FASTI were identified in the Logical Model (Figure 4 in the PSC) and in Arg 1.2.3. Principally, they are the FDPS, surveillance, meteorological data systems and CORT systems in adjacent sectors/ centres. The PSC identified generic categories of abnormalities in such systems. In essence they can all be considered in terms of either loss or corruption of the information that those systems exchange with FASTI.

It is also necessary to consider abnormalities in other ATM systems that do not normally interact directly with FASTI, and in the wider environment, but that could have 'knock-on' effects on safety. These have also been identified, in general terms, in the PSC – they can be considered under the headings of aircraft emergencies and failures, and human errors by pilots or errors made by controllers in tasks unrelated to FASTI.

What?

You will need to review and expand on these general descriptions of abnormalities, making them more specific to your own context and possibly adding to them.

How?

This is most effectively done by holding structured safety workshops (as described in the SAM) and by making use of historic experience – what types of abnormalities have been known to happen?

Who?

As the concern is with systems outside FASTI, it is important to bring in as wide a range of experience as possible, to complement your expertise in the FASTI domain itself. So, you should try to include pilots, and representatives from adjacent centres.

***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 safety if the events identified in Arg 1.4.1 occur, and to recover from them afterwards.

To satisfy this argument you will need to answer the question: '*if something goes wrong in another system, or environmental conditions change, how will our FASTI implementation respond safely?*'

The PSC defines the general types of Safety Requirements that will be needed for each of the general categories of abnormality. Essentially these SRs fall under three headings: detection of the abnormality, alerting the controller (or others, such as system engineers who need to know), and providing fallback (contingency) measures.

What?

Just as in Arg 1.4.1 you will have reviewed and expanded on the generic descriptions of the abnormalities, in this Argument you will need to assess their impacts and define more specific SRs, appropriate and proportionate to your particular context. You may also need to define Assumptions about certain external systems, where these lie outside your control.

Assumptions will require validation later in the Safety Case process or, if this is not possible, may place certain limitations on the use of FASTI.

How?

The basic process of developing the SRs is part of the PSSA process as described in the SAM. You should start the process within the brainstorming/ analysis sessions that you set up for Arg 1.4.1, involving a wide range of stakeholders. However, some of the issues can become quite complex and require detailed information – you will need to take these away for more detailed examination by a smaller group of specialists.

Where appropriate and practicable, the effects of external abnormalities should also be investigated as part of your simulations.

There are three general points to keep in mind when developing Safety Requirements related to external abnormalities:

- SRs related to external abnormalities are likely to overlap with those for detection, alerting and fallback of internal failures of the FASTI system (see Arg 1.5.2). So, for example, when designing a fallback that is proportionate to the risk, you should take account of the total probability of its being required: i.e. the sum of the probabilities resulting from both external abnormalities and internal failures
- External, interfacing systems such as FDPS support other ATM functions, not just those associated with FASTI. It may therefore be that some Safety Requirements on those systems are already in place, or that Assumptions about them have already been confirmed as valid. You should aim to identify additional, or different demands that FASTI will place on external systems, and define Safety Requirements or Assumptions only where necessary.
- FASTI may also have impacts (positive or negative) on fallbacks for existing systems that will remain in place after FASTI implementation. These also need to be identified and taken into account.

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. Loss or corruption of the checking systems need to addressed under Arg 1.5 and SR-FAS-13, as part of the consideration of reliability and integrity.

5.5 Arg 1.5: Risk from internal failures is sufficiently reduced

Arg 1.5 looks similar to Arg 1.4 in some ways, but differs in that it looks at internal failures (failures within the FASTI system), rather than external abnormalities (failures of other systems).

In the PSC, Arg 1.5 has been broken down into two sub-arguments dealing, respectively, with the identification of internal failures, and the definition of appropriate and proportionate Safety Requirements to reduce the associated risk. So the two key questions for you are: '*what could go wrong within FASTI that might affect its safety?'* and '*what do we need to do to prevent FASTI failing and/or to maintain a safe service if it does fail?'*

What?

You will need to review and expand on the material in the PSC, conducting an FHA/ PSSA process (as described in the SAM) to identify potential internal failures in your specific implementation of FASTI, to assess the risks they present, and to define appropriate and proportionate SRs by which such failures can be prevented, detected, alerted or mitigated against. Where appropriate and practicable, the effects of such failures should be investigated by simulation.

How?

Keep the following points in mind when developing Safety Requirements related to internal failures:

- 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, you will need 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.
- As already noted in the guidance on Arg 1.4.2, SRs related to external abnormalities and internal failures are likely to overlap – the same detection, alerting and fallback measures may apply to both. So, for example, when designing a fallback to be proportionate to the risk, you should take account of the total probability of its being required: i.e. the sum of the probabilities resulting from both external abnormalities and internal failures.
- The reliability and integrity of self-checking systems will need to be considered, as well as that of the primary information provision systems.

5.6 Arg 1.6: Suitability and sufficiency of the safety assessment

This argument requires you to answer the question: *'has our safety assessment process been conducted well, and have we done enough?*'

What?

To satisfy this argument, you need to justify the quality of your safety assessment process and the resulting Safety Case. You should describe the experience and expertise of the team that produced the Safety Case, the tools and techniques that you have used, and what review or auditing of the Safety Case has been done.

5.7 Arg 1.7: All Safety Requirements are realistic and demonstrable

Arg 1.7.1

This argument requires you to answer the question: *'have we set realistic targets for ourselves to ensure the safe implementation of our FASTI design?'*

What?

You need to show that you have considered the feasibility of your SRs.

How?

Look at each SR and review its feasibility in terms of hardware, software, people and procedures. Without going into details of the design as yet, ask whether it should be possible to implement the design safely against that SR, given available knowledge and technologies, and within the limits of normal human performance.

Who?

Talk to the relevant experts: designers, system integrators and, of course, the controllers.

Arg 1.7.2

This argument requires you to answer the question: *will it be possible to demonstrate that the SRs are satisfied in practice?'*

What?

To satisfy this Argument, you need to show that you have expressed each SR in terms that will make it as easy as possible to test whether or not it has been satisfied.

How?

Look at each SR and ask whether it presents a clear demand on whoever will have to implement the system. Try to imagine how it will look from their point of view. Is it clear what you are asking for? How will they know when they have satisfied it? Is the wording as precise as possible, and does it refer to parameters/ entities that can be measured and observed? As well as looking at each individual SR, you should review the set of SRs as a whole. Are there any overlaps or conflicts between SRs that could lead to confusion or difficulty in satisfying them?

For some Safety Requirements, however carefully you have worded them, deciding whether or not they have been satisfied is not straightforward, as it will be a matter of degree rather than answering a simple yes/no question. This is why SAME encourages you to take a 'System Assurance' approach: thinking in terms of the process – the activities that you will have to carry out in order to generate the Evidence with sufficient confidence, not just about the product or end-point – the Evidence itself. The Argument developed in the PSC has already made use of the guidance on the Assurance approach in SAME[7],[8], but you are

[7] In the current version of SAME, the assurance objectives and corresponding activities are, for Arg 1, generally to be addressed irrespective of the safety criticality of the system i.e. independent of the assigned Assurance Level (AL). However, the approach is still described as an Assurance approach because it deals with the process for generating Evidence, not just the product (the Evidence itself). Assurance Levels will be used more explicitly in Args 2, 3 and 4 to define different levels of rigour in the activities for various individual elements of the system, proportionate to their safety criticality.

[8] The assurance Objectives defined for Arg 1 in SAME are referred to in the PSC as lower-level Arguments (generally at the third or lower level of the hierarchy). For example, in Arg 1.1, assurance Objective i2 as defined in SAME is to 'ensure that a functional model has been clearly described, which completely and correctly interprets the Concept of Operations'. Satisfying this

encouraged to look back at SAME for yourself when reviewing and developing Arg 1.

Look out for updates to SAME (and the SAM) – the assurance approach is still relatively new and is likely to evolve further.

Who?

If you already know who will be in the implementation team, or have access to people with similar experience, ask them what they think (e.g. does the wording need to be amended or expanded to provide a clear test?)

objective requires the same activities and evidence as Arg 1.1.2 in the PSC: ‘A functional model has been developed that completely and correctly interprets the Concept of Operations’. In general, an assurance Objective can be reworded as an Argument and vice versa. The difference is simply a historic one, in that the PSC Safety Argument was largely developed before the Ed 0.2 of SAME.

6. DEVELOPING ARG 2 - SAFETY OF FASTI IMPLEMENTATION

Arg 2 is concerned with the safety of the implementation of FASTI, in which the high-level concept and design (from Arg 1) are developed in detail for your particular context and built into an actual system of hardware, software, trained people and procedures. Arg 2 aims to establish whether this ‘as built’ system can achieve the required level of safety.

The first three sub-arguments cover the satisfaction of the Safety Requirements identified in the Definition stage (Arg 2.1), the possibility that new hazards are introduced when the system elements are combined (Arg 2.2) and making the best choice from amongst the various possible physical implementation options (Arg 2.3). In the following sections we summarise the proposed argument structure from the PSC, identify the key questions and give ‘what/ who/ when’ guidance on how to answer them.

Args 2.4 to 2.7 are concerned with the practical processes of procurement, construction, integration and commissioning. We have not provided any specific further Guidance on these four Arguments (beyond what is already in the PSC), as these are largely concerned with the internal management processes of each ANSP. However it is worth noting that experience suggests the following are critical success factors for these processes [Ref - *Good Practice Guidelines for FASTI with a Focus on Human Factors and Managing the Transition* [Ref. 28].

- Is enough time, resource and money available?
- Is the right team in place to manage implementation?
- Is there staff acceptance?
- Are users aware of the potential benefits that implementation will bring?
- Do you have a good relationship with your (potential) supplier?

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

This Argument aims to show that your concept and high-level design for FASTI, as embodied in the SRs identified in Arg 1, have been included in the detailed design and the actual implemented system. SRs are requirements on the ongoing functionality, performance, reliability or integrity of the operational system. They represent a formalised statement of your intentions for FASTI (providing a clear basis for procurement, amongst other things) and this argument is therefore important in preventing ‘requirements creep’ – the gradual compromising or downgrading of intended benefits that can often occur when project timescales or budgets become stretched.

The key question is *‘have we done what we said we would do in Arg 1 in order to ensure the safe implementation of FASTI?’*

What?

In principle, satisfying this argument is a relatively straightforward process of checking off each SR from Arg 1 as it is implemented.

How?

But in practice it is at this stage that ANSPs often encounter a major problem: the limited ability of practicable validation and verification methods to show, with sufficient confidence, that the Safety Requirements have actually been satisfied. 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.

To address this problem, EUROCONTROL has been developing an assurance-based approach as a pragmatic means of demonstrating the satisfaction of Safety Integrity Requirements (and in some cases, Functional Safety Requirements) in the main elements of the physical system: software, procedures and humans.

You can find guidance on the AL process in the SAM. In brief, it requires you to assign an Assurance Level (AL) on a four-point scale to each element of the system, based on an assessment of its safety-criticality (broadly speaking, 'how bad would it be if it failed'). AL1 is the highest criticality, AL4 the lowest. The assigned AL then determines the assurance processes to be applied in implementing that element – the extent and rigour of the process being proportionate to its safety-criticality. The assurance processes are defined in the SAM guidance in terms of objectives (what you must do), activities (how to do it) and evidence requirements.

Currently the SAM specifies assurance levels and processes for software (SWAL), and procedures (PAL). A similar process for human elements of the system (HAL) is under development. While the detailed process is not yet fully defined or readily applicable to all types of system and element[9], you should still find it helpful to follow the general principle: that the time and effort you put into achieving the SRs in implementation (and indeed in the transition and operation stages too) should be proportionate to the safety criticality of the system elements concerned.

Who?

The AL process needs to be guided by people with experience with formal safety assessment methods, and to have input from people with experience in the related operational and technical disciplines

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

When system elements are combined and begin to interact in complex ways, it is possible that new hazards may arise, as emergent properties that were not foreseen in the development of Arg 1. It is therefore not sufficient merely to check off the SRs identified in Arg 1; the safety of the whole implemented system also needs to be demonstrated.

What?

Simulations, including dynamic simulations, should be performed to check the safety of the whole system in practice and identify such emergent properties.

[9] You should look out for updates to SAME, which is continuing to develop the assurance approach

When?

It may be more efficient and effective if these simulations are carried out once the system is fully implemented and ready for ‘pre-operational’ trials during the Transition stage (Arg 3.1). Deciding when to conduct simulations always involves a balance between the dangers of doing it:

- too early (when the system design is still evolving significantly, such that the results do not accurately reflect the final system) and
- too late (when decisions have already been made and it will be difficult and costly to change anything if problems do arise).

Bottom-up analytical techniques such as HAZOP or FMEA may also help in looking for potential common cause failures that affect more than one element of the system.

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

There will often be more than one way of implementing FASTI and integrating with existing systems.

What?

In your feasibility studies and option selection, you need to consider safety aspects thoroughly and ensure that the choice has been made with due regard to safety. This is part of satisfying **Cr02**: the requirement to minimise risk.

7. SAFETY OF FASTI TRANSITION (ARG 3)

This argument aims to show that transition from the old to the new system is performed safely. You will need to show how the built system, whose safety was proven under Arg 2, can be brought into operational use, without affecting the safety (or continuity) of the on-going ATM service, and whether the necessary preparations for bringing the system into service, and for supporting it in service, have been completed.

Keep in mind that transition will include provision of resources (people, equipment spares, maintenance facilities etc), arrangements for safety management, change management, configuration control etc as well as the arguments related to the ‘core’ of FASTI people, procedures and equipment that we have focussed on up to this point. Appendix C provides some additional guidance on these practical aspects of managing change.

At the core of this stage is the second part of the SSA process, details of which are given in the SAM. It is important to note that the current version of SAM (Version 2.1) provides guidance mainly on what we have called the failure approach. Therefore, the SAM should be read in conjunction with the following text and any available future guidance from EUROCONTROL’s SAME work.

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), and hazards in the transition process itself (Arg 3.3). Args 3.4 – 3.9 then cover the practical steps in final preparation for operation.

Note that you will not necessarily carry out these final preparations in the order implied by Args 3.4 to 3.9. In practice these steps are quite interdependent and there is likely to be some iteration between them. The detailed sequencing of, and dependencies between, these steps – and hence the order in which you develop the safety arguments – will also be affected by the specifics of your planned programme for roll-out to operational use.

It may often be difficult to show conclusively that a sub-argument within Arg 3 has been satisfied or not; the Assurance Level approach, as described under Arg 2.1, can be extended to Arg 3 as well. It involves showing that the process has been sufficiently rigorous rather than the final product.

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

Pre-FASTI situations will vary across ANSPs and States. For the purposes of the PSC, a 'typical' baseline pre-FASTI situation was defined.

What?

If you start from a different baseline, you will need to adapt and develop your Safety Case accordingly. For example, if you need to implement some enabling measures to come up to the baseline, you will 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*

What?

You should conduct pre-operational simulations and user trials, including dynamic simulations, to check how the fully-developed FASTI system will work safely in practice. This should include effects on neighbouring, non-FASTI airspace.

As part of the validation, you should carry out final user tests and refinement of the Operations Manual and Procedures.

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

This argument requires you to answer the question: '*have we made sure that there will be no additional risks when we change from the old system to the new one?*'

What?

To satisfy this Argument, you need to provide evidence of a systematic consideration of the risks that could be introduced during the transition. All hazards associated with switch-over from the old systems to the new systems must be assessed and mitigated sufficiently.

How?

You should carry out hazard identification and risk assessment studies (a sort of FHA/PSSA/SSA of the transition) 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.

This is an example of where you could use the Assurance Level approach (see Arg 2.1). It is impossible to provide absolute proof that all hazards have been identified – there is always the possibility that something has been overlooked. But you can demonstrate the rigour with which you have carried out hazard identification in terms of – for example – what activities you have undertaken (such as brainstorming, FMEA, analysis of past incidents etc) and the types of experience and expertise brought to the process.

This assessment should result in the development of robust additional procedures, allocation of responsibilities and training, and the briefing of personnel necessary to prevent (as far as possible) things going wrong, or take appropriate action should something go wrong.

Arg 3.4 *Safety-related training has been achieved*

This argument requires you to answer the question: '*have we trained all necessary staff to ensure that FASTI operates safely?*'

What?

To satisfy this Argument, you need to provide evidence of the training you have provided, including the rationale for the content of that training and a register of who has been trained, and the training of the trainers.

It 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. Engineering and support staff may also require training.

It is important that the training you provide ensures understanding of the basis and intent of FASTI tools as well as practical 'how to' instruction. This will support correct expectations and use of tools – for example by helping controllers to appreciate the importance of updating the system.

Training should be linked to and reinforce the operational procedures and working methods that you need in order to realise the benefits of FASTI (see Arg 3.5 below). It should not just involve 'how to use the HMI', nor should there be too much reliance on user manuals.

Ensure that training sets up appropriate expectations of the tools and degree of trust. Refer back to your automation strategy as defined in Arg 1.2.1.5 and ensure that these expectations match the intended degree of reliance. At this stage you can be more specific and detailed about this – e,g. how will variations between individual controllers be accommodated?

Further guidance can be found in the EUROCONTROL Human Factors Case approach [Ref 27] and the SHAPE project [Ref 31] which gives guidance on training to build up trust.

Take account of the possibility of controllers being trained on the new system, but still having the mindset required by the old one, or of 'interference' from the old mindset or behaviours.

Be aware of the danger of training on the system before it is stable. If changes have to be made then training will have to be repeated, and trust in the programme may be affected. Systems used for training should behave as you would expect them to once operational. However, training should not be at the 'last minute' – allow time to consider feedback properly and make any necessary changes in, for example, procedures.

Some ANSPs may have licensing requirements for controllers using the new tools, and/ or formal schemes for assessing competency. Training should be planned around the requirements of any such licensing/ competency schemes, and the safety argument should reference these schemes appropriately.

Refresher training should be planned and scheduled at appropriate intervals.

Arg 3.5 *Working methods are safe and appropriate*

As part of Arg 1.2.1.5, you will already have defined the level and scope of automation, and associated working methods and procedures. However, at that time, it is unlikely that you will have had a clear enough idea of the context and system details to define working methods very precisely. This argument is concerned with refining the working methods and ensuring that controllers will actually use the new system safely and as intended.

What?

You need to ensure that the working methods and procedures are actually safe and appropriate and that they will be used as intended by the controllers. You should therefore review the working methods in more detail, in the light of what you now know about the practicalities of operating the system.

For example, consider whether TC and PC working methods are well-matched in speed of working, competencies required, and PC/ TC expectations of each other.

Results from the pre-operational validation (Arg 3.2) and feedback received during training (Arg 3.4) or shadow-mode operation (Arg 3.7), will feed into this argument.

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

This argument requires you to answer the question: '*can everybody involved in the new system access the information they need?*' The types of information required will include the operational procedures, engineering procedures, and any associated airspace or ATM procedural changes that may affect airspace users.

What?

To satisfy this Argument, you need to describe how you have made sure that these sources of information are easily available to those who need them.

How?

You should consider making this information available on your intranet, to assist dissemination, as well as in hard copy form in the operations room.

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

Shadow-mode operations will enable you to make a further, final check on the safety (and operability) of FASTI before going live. You should monitor, in particular, user acceptance and adaptation to new practices, roles, teamwork and adherence to procedures, and modify the system or training if required.

What?

To satisfy this Argument, you will need to provide evidence of the shadow-mode trials you have undertaken, their results, and your rationale for concluding that this has established safety in a realistic context.

Some ANSPs may consider shadow-mode trials as part of pre-operational validation (Arg 3.2). But however your validation is phased and planned, and whatever you call the various stages, the important point is that by running FASTI alongside real operations, a more realistic context is established.

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

What?

Systems that will no longer be required should be safely removed. This includes, for example, uninstalling software. If appropriate, some old systems may need to be left in place as fallback. If so, you will need to ensure that the associated procedures remain accessible and that controller training maintains their ability to use these systems.

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

This argument requires you to answer the question: *'did we achieve everything as planned on O-date, and immediately after?'*

What?

You will need to describe the successful and safe implementation of the new system on O-date.

How?

Indicators of successful implementation may include how long it takes controllers to begin using the new tools fully, passing a certain number of movements using the new system, and positive feedback from controllers. Safety indicators may include the number of STCA alerts, and whether any backup systems needed to be used.

8. SAFETY OF FASTI OPERATION (ARG 4)

Arg 4 aims to show that the operational use of the system, including its maintenance and updating, is, and will continue to be, acceptably safe. This is an essential check of the results of the previous stages of the Safety Case and the safety assessment (FHA, PSSA, and SSA), all of which are necessarily based on prediction. In essence, you will need to provide Evidence that the whole of the preceding Argument (the overall Argument with its Criteria and Assumptions etc, and Arguments 1, 2 and 3) is valid in practice.

The technical core of this phase is the last (third) part of the SSA process, details of which are given in the SAM. The current version of SAM (Version 2.1) provides guidance mainly on what we have called the failure approach. Therefore, the SAM should be read in conjunction with the following text and any available future guidance in SAME.

It may often be difficult to show conclusively that a sub-argument within Arg 4 has been satisfied or not; the Assurance Level approach, as described under Arg 2.1, can be extended to Arg 4 as well. It involves showing that the process has been sufficiently rigorous rather than the final product.

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

In order to satisfy this Argument, you need to provide evidence that the operational system is working safely in practice.

What?

You will need to monitor the safety performance of the system during its operation, especially to establish the ongoing safety of aspects that can only realistically be checked in operational service.

How?

All safety-related incidents must be reported, investigated and the appropriate corrective action taken. This should be part of your normal incident reporting system, but you should consider whether any additional features need to be put in place for controllers to report any specific difficulties with FASTI. For example, if you use keywords to categorise different types of incident or factors, are these keywords appropriate and informative for FASTI-related problems?

The indicators of safe implementation that you should monitor include the following:

- Occurrence of incidents (re-use, with adaptation if required, the safety metrics defined for use in simulation in Arg 1.3.3)
- These indicators may be useful in ways other than as pure safety indicators. For example, MTCD alerts may help you identify sectors that have more conflicts than others.
- Usability, workload, roles, teamwork. Set up feedback schemes and/ or observations to assess how controllers are adapting to new work methods. Are they using the new system as intended? Do real work practices match written procedures? Feedback may be expected

especially regarding tuning of system parameters (e.g. to optimise the false alert rate) and training ('what you wish you had known').

It is good to have a training instructor available in the early days of operation for questions, and as a reporting point for any comments and concerns.

Refresher training should be conducted at sufficiently frequent intervals.

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

This argument requires you to answer the question: '*are we continually reviewing and maintaining the system?*'

To satisfy this Argument, you need to provide evidence of the maintenance and upgrade/update activities that are undertaken, showing that these are part of a structured and planned approach to the overall maintenance of the new system.

What?

Safety assessments must be carried out for any maintenance, upgrades or other planned interventions, to ensure that any risks that may be introduced are identified and are acceptable.

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

Your Safety Case is of course a key element in ensuring safe continued operation when changes are made. Documenting both what the system is, and why it is like that, will help to avoid the danger that changes will be made without full understanding of their safety implications.

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

This argument requires you to answer the questions: '*are we reviewing the system when things change, and adapting it where necessary in response to those changes?*'

What?

To satisfy this Argument, you need to show that there is a regular review of the system's environment, identification of relevant changes, and subsequent assessment and change where necessary in the design or use of FASTI.

How?

You should have a systematic process for monitoring changes that may affect the system. Consider for example changes in traffic and airspace, and the introduction of other new systems, and look in particular at areas that may change the validity of your Assumptions. This should be part of your wider SMS, providing for regular monitoring and review of changes.

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

This argument requires you to answer the question*: 'have we documented everything that may be needed by designers of the new system, and made this documentation easily available?'*

What?

The safety of decommissioning is actually outside the scope of FASTI, in that any safety considerations should be identified in the Safety Case process for the new system, assuming that your SMS is operating properly.

However, you can help to avoid future problems by ensuring that the Safety Case is regularly reviewed, kept up-to-date, and that it and supporting information about the system are stored in an accessible form and place. In particular, it is important that documentation explaining the 'why' as well as the 'what' of FASTI, i.e. the design and its rationale as covered in Arg 1, is adequate and readily accessible. Without this, there is a danger that the importance of features being replaced or removed will not be appreciated. Organisations can have a very short memory.

9. CONCLUDING YOUR SAFETY CASE

9.1 Assumptions

In the PSC, these have been written to reflect a typical implementation of FASTI and should not need to undergo major changes. However, you are encouraged to review these assumptions to ensure that they reflect your own context, needs and Concept of Operations and any more detailed Assumptions that are still outstanding during operation.

9.2 Issues

Safety Issues are used to note outstanding matters to be addressed during the process of developing the Safety Case, before the Claim (that the implementation of FASTI is safe) can be accepted. They are used to drive a 'to do' list – what needs to be done, who will do it and the timescale in which this will occur.

By definition, once the Safety Case is complete for operation, there should be no remaining Issues. You should check that this is the case.

9.3 Limitations

At various points in the Safety Argument, you are likely to have found areas in which limits or constraints on the operation of FASTI exist, or need to be imposed. This section of the Safety Case should summarise these limitations in one place, to provide a clear statement for users of what FASTI can and cannot be expected to do. You could group them according to the areas of operation that are affected in each case.

9.4 Conclusions

Use this section to summarise your Safety Case. You should be able to state that the overall claim has been satisfied, but briefly remind readers of the scope of the document, the particular operational context to which it has been applied, and the assumptions and limitations.

9.5 Recommendations

ANSPs should use this section to specify how their Safety Case should be distributed, used, reviewed, and updated. There should be no recommendations regarding FASTI itself, as these should already have been addressed in the appropriate arguments.

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 Preliminary Safety Case, Edition 1.1, 3 Sep 2008.
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: ORGANISATIONAL ERROR IN IMPLEMENTING NEW SYSTEMS

Organisational error concepts

Most people are familiar with the concept of human error now, after many years of newspaper stories and accident reports blaming incidents on the actions of an individual. For example, a man employed by Network Rail (the UK railway infrastructure provider) was arrested by police in connection with a train crash in Cumbria, UK, on February 23rd 2007, which left 1 woman dead and many injured (‘Network Rail worker arrested over crash that killed woman’, The Guardian, Saturday July 14, 2007). This incident is unlikely to have been the result of one man’s actions, however. It is more likely that there were a succession of mistakes in the training, selection, supervision and management of this one employee, as well as the systems and procedures that were in place to ensure quality and safety standards.

Active errors (or unsafe acts) are associated with the actions of those involved in an incident or accident, and result in effects that are apparent within a short timeframe. However, incidents may often result from operators inheriting a system that contains latent problems or weaknesses that make it easier for hazards to manifest. These weaknesses or latent errors may include poor maintenance, mistakes at the design stage, or ill-advised decision-making at management level. If required, latent errors can be categorised further, for example, as either unsafe conditions (including the condition of operators, environmental conditions and other personnel factors) or unsafe supervisory practices (including inadequate supervision, supervisory violations, planned inappropriate operations and failure to correct a problem[i]).

Addressing and preferably preventing latent errors is believed to be a powerful method of improving safety. Furthermore, in the implementation of a new system, ANSPs have a special opportunity and responsibility to avoid introducing latent failures Addressing latent errors will not prevent operators from making mistakes in every instance; however, it can decrease the severity or frequency of those mistakes, and may increase the effectiveness of the barriers to, and mitigators of, hazards.

Latent errors (either as a group, or divided into unsafe conditions and unsafe supervisory practices as previously suggested) may also be categorised as either errors of commission (doing the wrong thing) or errors of omission (failing to do the right thing[ii]). See below for examples illustrating how these terms might be used in the analysis of error in an organization providing ATM services.

	Active error	Latent error
Error of commission	The controller makes a wrong input into the system	The organisation allows an inexperienced controller to become an instructor
Error of omission	The controller does not notice an alert	The organisation fails to create a procedure to ensure communication between those involved in maintaining the FASTI tools, and the controllers who depend upon them

There are a number of different frameworks that you may use to consider the potential for error at an organisational level during the implementation of FASTI.

These frameworks may be used to provide systematic assurance that such issues have been considered, discussed and addressed during the course of completing the Safety Case. You are encouraged to choose elements from these approaches in order to develop your own method, based upon your particular needs and context.

Managing Change

When a new system or technology is introduced into an organisation, change will be experienced by employees at every level, and this will manifest itself in other systems, procedures and documentation across the organisation. The transition period is the name given to the period of change from one system or way of working to another. This period of change, when new policies and procedures and systems are created, is a time when latent errors may be created. However, change continues after the transition period, and after FASTI has been implemented. There are, in effect, three aspects of change:

- The change in procedures and working practices and environment (the transition to the new system)
- The increased automation and consequent change to the working profile of controllers (the system itself)
- Increased productivity and/or capacity (change resulting from the introduction of the new system)

Organisations need to continually ask themselves whether they are managing the changes in an effective and safe manner, and ensure there are sufficient opportunities to stop and evaluate the process to make sure it is still on track. Managing the change process effectively may encourage better engagement and communication, allowing potential organisational safety issues to come to light and receive proper consideration and hence reducing the risk from latent error.

Using best practice guidance and lessons learnt by other ANSPs

A Safe Approach to Transition (EUROCONTROL, 2005[iii]) suggests the key safety elements to be considered during the Transition period to operational implementation of an ATM system or sub-system, based on advice gained from a number of ANSPs who have been through major transitions.

The report includes a discussion of “indirect” safety aspects such as commercial time pressure which can lead to a mentality and culture that places greater importance on meeting the target date for operation, than on considering safety. This may lead to latent errors of commission and omission including:

- Cutting corners when testing;
- Pressure to downplay the severity of an identified hazard in order not to hold up the project;
- Pushing the responsibility for certain areas of risk onto future training and procedural requirements instead of taking the time to deal with them in the design and planning phases;
- Allocating insufficient resources to safety;
- Failing to give safety an appropriately high emphasis on the agenda and in the status of those who are charged with ensuring it;

- Failing to take the time to pursue good ideas; and
- Failing to consider all elements of the system, and the inter-dependencies of those elements, due to a reliance on external safety contractors who may only deal with one small part of the Safety Case.

EUROCONTROL's Good Practice Guidelines[iv] identified a number of "critical success factors" based on data collected from ten ANSPs in Europe who have experience of implementing new tools. These are:

- State clear project aims and objectives
- Get the system specification right
- Allocate appropriate time, resources and money
- Create the right team
- Get staff acceptance
- Communicate the benefits of the change to the users
- Establish good communication and a trusting relationship with your supplier

More generally, you may like to refer to benchmarking studies[v] to use the lessons learnt by other ANSPs.

Structuring your approach around theories of change management

There are many theories and models suggesting ways in which to manage change. Kotter (1996)[vi], for example, suggested that there were eight steps involved in the successful management of organisational change. These are presented below with some suggestions as to how they could be adapted for the specific example of implementing an ATM system.

- Establish a sense of urgency – by presenting the benefits of FASTI to employees, it would be possible to instil in them the view that the change to this new system is necessary and positive.
- Form a powerful core team to drive change – consider the range of interests that should be represented. These could potentially include controllers; supervisors; trainers; maintainers of the hardware and software; recruiting/ marketing functions; and legal viewpoints although each ANSP may have a different group of stakeholders that should be involved.
- Create a vision and strategy – this should be clearly worded and relevant, and will guide the entire transition process. It may be particularly important to ensure that everyone knows what the objectives of the change are with regard to the balance between increasing capacity/ improving safety.
- Communicate the vision – the vision should be communicated as often, and as clearly as possible to every employee.
- Empower others to act on the vision – for example, when FASTI is operational, how can managers and supervisors ensure that old approaches or work-arounds are not used?
- Generate short-term wins – recognize and celebrate the achievement of interim goals.

- Consolidate improvements and produce still more change – some ANSPs may develop new systems and procedures in other, related areas as a result of the successful implementation of FASTI, using the momentum to make further improvements or explore other innovations.
- Institutionalize the new approach - make FASTI, and the use of automation to provide ATM services, a clear part of the organisational culture. This may be difficult as the current culture may be strongly invested in the mental abilities and skill of controllers. Controllers themselves may feel that their position is being deskilled, and may become unsatisfied, and there will almost certainly be a point in time when the organisation contains a mix of employees from "before" and "after" the change occurs. Recruitment may well move to focus on different skill profiles and attitudes toward technology and there may be an extended transition period while the two groups of employees coexist.

You might like to refer to this kind of framework to guide the transition to FASTI and encourage a positive and safety-aware culture, lessening the possibility that latent errors will go unseen, unreported, or uncorrected.

Summary

Consider the type of culture in your organisation, the way in which existing systems are managed, and the complexity of your operations in deciding upon the best way to manage the implementation of FASTI. The way in which this process is approached will depend on the culture of your organisation.

An important aspect of change is the effect it can have on employees, particularly if they feel that their role is being deskilled or devalued in some way. This is particularly relevant for ANSPs seeking to implement FASTI. Communication with controllers should be clear and straightforward, outlining all planned changes and explaining the reasons for these changes. Managers should also seek feedback from controllers about whether the changes are working, or whether there are any problems.

Controllers may have particular issues regarding the reliability of FASTI, and so you need to consider providing their controllers with as much information as is requested. They may also need reassurance regarding their role and job security, and there may be a need to establish support services to address any particular concerns that emerge during the change process.

You should also ensure that the change process does not have a negative impact on the performance or safety standards of other systems – that all of the attention is not focused upon the implementation of FASTI to the detriment of other concerns.

References – Appendix C

i. Reason, J. (2003). Human Error. Cambridge: Cambridge University Press.

ii. Matthews, G., Davies, D.R., Westerman, S.J. & Stammers, R.B. (2000) Chapter 8: Human Error. *In* Human Performance: Cognition, Stress and Individual Differences. (pp141-160). Hove: Psychology Press.

iii. EUROCONTROL. A Safe Approach to Transition: Key Elements for Transition Success, 2005, Report No. 405

iv. EUROCONTROL. Good Practice Guidelines for FASTI with a Focus on Human Factors and Managing the Transition. Released Issue: 18/06/2007

v. EC. Study on benchmarking for best practices in Air Traffic Management in European Union candidate states, 2003)

vi. Kotter, John P. (1996) Leading Change. Boston: Harvard Business School Press.