

EUROCONTROL



**EUROCONTROL Guidance
Material for Short Term Conflict
Alert
Appendix B-1: Safety Argument
for STCA System**

Edition Number	:	1.0
Edition Date	:	14 December 2006
Status	:	Released Issue
Intended for	:	EATM Stakeholders



DOCUMENT CHARACTERISTICS

TITLE			
EUROCONTROL Guidance Material for Short Term Conflict Alert			
Appendix B-1: Safety Argument for STCA System			
	ALDA Reference: 06/12/14-23		
Document Identifier	Edition Number: 1.0		
	Edition Date: 14 December 2006		
Abstract			
<p>This document is the first of a set of three documents the purpose of which is to provide guidance material for ANSPs to assure their own implementations of STCA in accordance with the EUROCONTROL Specification for Short Term Conflict Alert (STCA) in the ECAC area. This document describes a possible Safety Argument.</p>			
Keywords			
Safety Nets	Safety Case		
STCA			
Safety Argument			
Safety Plan			
Contact Person(s)		Tel	Unit
Ben Bakker		+32 2 72 91346	DAP/ATS

STATUS, AUDIENCE AND ACCESSIBILITY			
Status	Intended for	Accessible via	
Working Draft	<input type="checkbox"/> General Public	<input type="checkbox"/> Intranet	<input type="checkbox"/>
Draft	<input type="checkbox"/> EATM Stakeholders	<input checked="" type="checkbox"/> Extranet	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/> Restricted Audience	<input type="checkbox"/> Internet (www.eurocontrol.int)	<input checked="" type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>	<i>Printed & electronic copies of the document can be obtained from ALDA (see page iii)</i>	

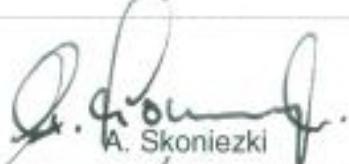
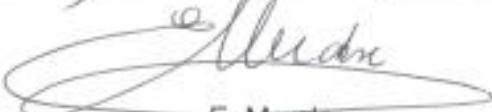
ELECTRONIC SOURCE			
Path: \\HHBRUNA02\bakkerb\$\STCA			
Host System	Software	Size	
Windows_NT	Microsoft Word 10.0	323 Kb	

EUROCONTROL Agency, Library Documentation and Archives (ALDA)
EUROCONTROL Headquarters (50.703)
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 11 52
E-mail: publications@eurocontrol.int

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Technical Manager	 B. Bakker	14.12.06
ATC Domain Manager	 M. Griffin	18.12.06
ESP Programme Manager	 T. Licu	18.12.06
Head of DAP/ATS	 P. Dias	18.12.06
Head of DAP/SSH	 A. Skoniecki	18/12/2006
Deputy Director ATM Programmes	 E. Merckx	18/12/2006

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	17-5-2005		Draft for review by SPIN Task Force	All
0.2	10-8-2006		Results from review incorporated; status raised to proposed issue	All
1.0	14-12-2006	06/12/14-23	Formatting changes	All

CONTENTS

DOCUMENT CHARACTERISTICS.....	ii
DOCUMENT APPROVAL.....	iii
DOCUMENT CHANGE RECORD.....	iv
EXECUTIVE SUMMARY.....	1
1. INTRODUCTION.....	3
2. Purpose of this Document.....	3
3. Scope	4
4. OVERALL SAFETY ARGUMENT	4
4.1 Symbols Used	4
4.2 Overall Argument structure	5
4.3 Arg 0 Main Claim.....	6
4.4 Criteria.....	6
4.5 Context.....	6
4.6 Assumptions.....	7
4.7 Strategy.....	7
4.8 Arg 1 STCA functional & performance requirements are specified which if implemented can be expected to meet the primary safety objective for STCA & Cr 01.....	7
4.9 Arg 2 Safety requirements are specified which if implemented can be expected to mitigate against potential hazards and satisfy Cr02	9
4.10 Arg 3 The System Design correctly implements the functional, performance and safety Requirements	10
4.11 Arg 4 The risks associated with deploying the system have been reduced to a tolerable level	11
4.11.1 Arg 4.1 The system is acceptable for transfer to operations.....	12
4.11.2 Arg 4.2 The system is operated, maintained and monitored correctly.....	12

EXECUTIVE SUMMARY

It is Safety Management best practice and an ESSAR4 requirement to ensure that all new safety related ATM systems or changes to the existing system will meet their safety objectives and safety requirements. ANSPs and National Safety Authorities will need documented assurance that this is the case before deploying the new or changed system in operation. Typically, the assurance is presented as a safety case.

This document is one of a set of three documents the purpose of which is to provide guidance material for ANSPs to assure their own implementations of STCA in accordance with the EUROCONTROL Specification. The document set includes:

- Safety Argument for Short Term Conflict Alert [This document]
- Generic Safety Plan for the implementation of STCA
- Outline Safety Case for STCA

The documented assurance should contain the evidence, arguments and assumptions as to why a system is safe to deploy. The process of developing and acquiring the necessary assurance is considerably enhanced if the assurance arguments are set out clearly from the outset and ideally during the system definition phase of a project.

A generic safety argument for STCA is set out in this document and it is intended for use by ANSPs in developing assurance for STCA applications.

The argument should follow a logical structure, and be complete regarding the scope of the system, its environment, and any assumptions that have to be taken into account regarding these.

Development and review of safety argument is aided by the use of a graphical presentation rather than just text alone. It is easier to follow the logic of the argument in graphical form and to check it for completeness and correctness. Such an approach is employed in this document, based on a EUROCONTROL adaptation of Goal Structured Notation [GSN].

ANSPs may find it convenient to present their argument as a stand-alone document initially, as is the case with this document. However, the argument will ultimately form part of the safety case document and the stand-alone version will then become defunct.

The evidence required to support the argument is identified in this document. The activities necessary to obtain this evidence should be scheduled in a safety plan. The combination of the safety argument and the output from the safety plan should provide all that is necessary to make a safety case.

1. INTRODUCTION

Short Term Conflict Alert (STCA) is a ground-based safety net intended to assist the controller in maintaining separation between controlled flights by generating, in a timely manner, an alert of a potential infringement of separation minima.

The European Convergence and Implementation Plan (ECIP) contains a pan-European Objective (ATC02.2) for ECAC-wide standardisation of STCA in accordance with the EUROCONTROL Specification for Short Term Conflict Alert. This Specification contains the minimum requirements for development, configuration and use of STCA, and serves as reference for the detailed safety work that is needed for safety assurance of STCA and for ESARR 4 compliance.

The detailed safety work must be undertaken in accordance with European and National regulations and directives, which may refer to the EUROCONTROL recommended methodologies and practices. The current document is part of a set of documents that have been produced under contract by NATS, to serve as guidance material for carrying out the detailed safety work using the EUROCONTROL recommended methodologies and practices.

The set of documents consists of:

- Safety Argument for STCA
- Generic Safety Plan for STCA Implementation
- Outline Safety Case for STCA

2. PURPOSE OF THIS DOCUMENT

The document contains a generic argument intended to be used by ANSPs in developing safety assurance for STCA applications. The aim is to aid ANSPs in reasoning about what is necessary by way of assurance in claiming that the STCA system will benefit safety and to reveal the logic behind such reasoning. The logic of the argument is presented graphically so that it can be reviewed easily for completeness and correctness. The evidence required to support the argument is identified. The safety argument and associated evidence are essential content for a safety case¹.

¹ A Safety Case is defined by the EUROCONTROL SCDM [1] as "...the **documented** assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. It is primarily the means by which those who are accountable for service provision or projects assure **themselves** that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety"

ANSPs may find it useful to develop their argument in a stand-alone document initially, as with this document. One advantage of doing so is that it could be used as an early deliverable to their regulator when seeking prior approval for their planned assurance strategy. However, the argument will ultimately form part of the safety case document and the stand-alone version will then become defunct.

3. SCOPE

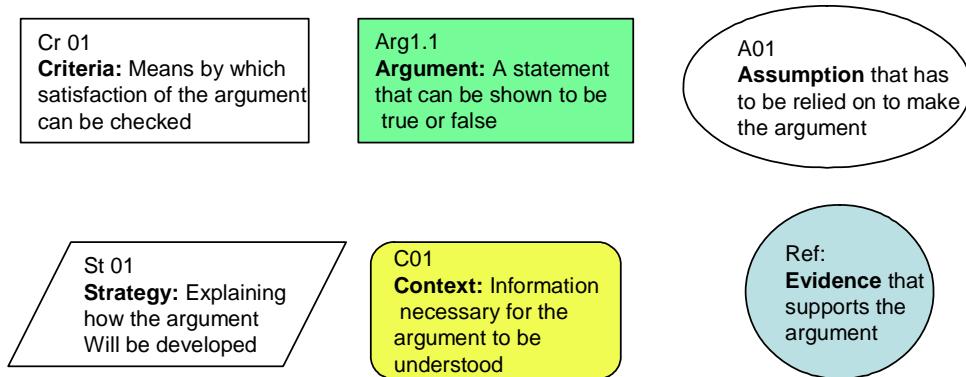
The safety argument applies to Short Term Conflict Alert, STCA. It encompasses all stages of a system lifecycle from definition of the operational concept through to operation and maintenance. It includes the safety assessment processes. The document should be read in conjunction with the Generic Safety Plan for Implementation of STCA.

The justification for implementing STCA is founded on the premise that STCA will provide a substantive safety benefit in ATM operations. Therefore, the argument set out in this document is not limited to showing that STCA is safe to deploy – i.e. does not cause an unacceptable increase in risk - but has been extended to include the claim that STCA will actually provide a substantial safety benefit – i.e. will reduce risk.

4. OVERALL SAFETY ARGUMENT

4.1 Symbols Used

The argument is represented graphically in GSN using the following symbols:



4.2 Overall Argument structure

The overall argument is structured as shown in Figure A below. The sub arguments are mapped on to the STCA development phases from system definition through to operation and maintenance. This is to enable the planned safety assurance activities to be linked closely to the system development and the safety case development.

Each of the arguments may be regarded as a claim about the system that has to be satisfied in order to make a safety case.

The main claim is dependent on the following four part argument comprising Arg 1 to Arg 4: The sub arguments are developed in the GSN Figures B1 to B4, as indicated.

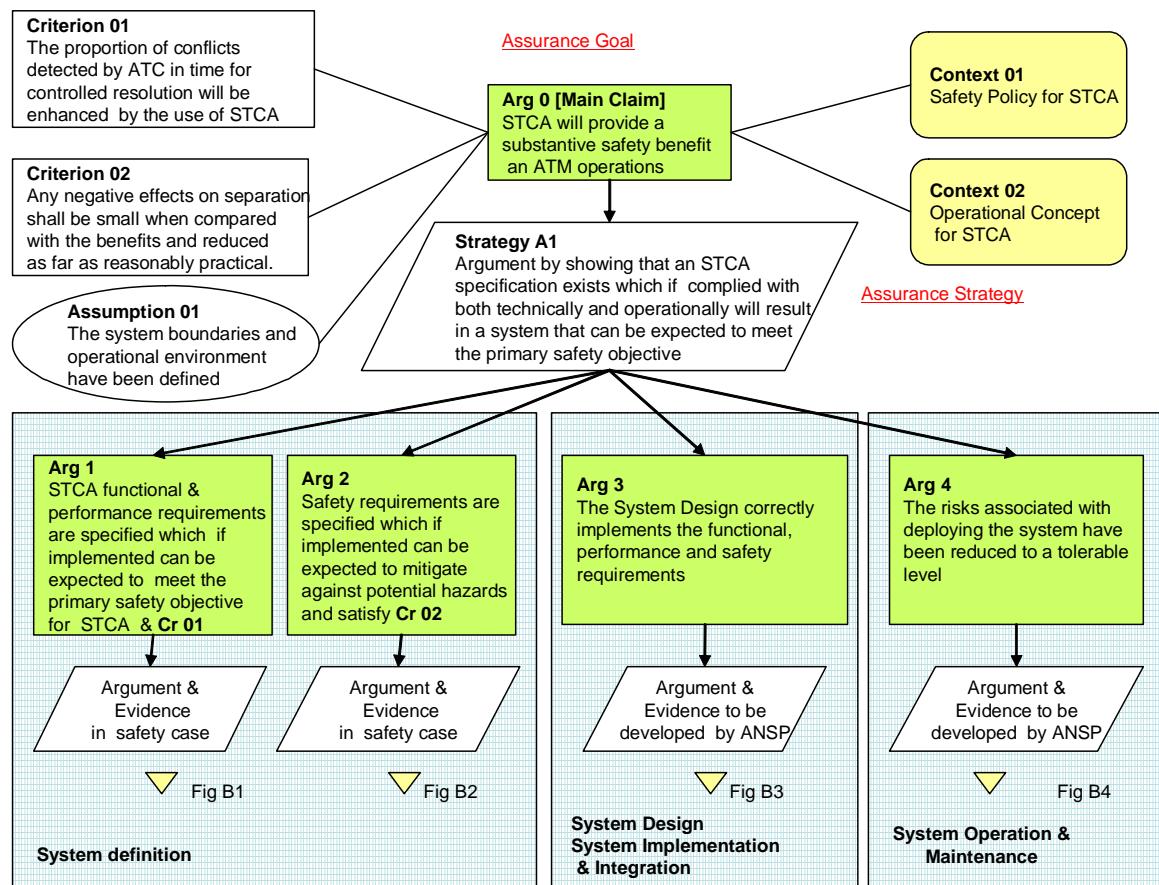


FIGURE A MAIN ARGUMENT STRUCTURE

4.3 Arg 0 Main Claim

The main claim to be argued is that “STCA will provide a substantive net safety benefit in ATM operations”. The underlying argument structure is the means by which the supporting evidence is linked to the claim.

4.4 Criteria

The criteria for deciding what will constitute “a substantive safety benefit” in making the argument have to be established at the outset.

The first criterion (**CRITERION 01**) adopted is that “the proportion of conflicts detected by the Controller in time for controller resolution will be enhanced by the use of STCA” - i.e. STCA will make a significant contribution to safety.

A second and equally important criterion, (**CRITERION 02**) is that “any negative effects on safety shall be small compared with the safety benefit and reduced as far as reasonably practical”.

These criteria provide a basis for a relative safety argument whereby the safety benefit (e.g. in terms of number of conflict alerts) should significantly outweigh the negative effects (e.g. the number of nuisance alerts). It is a matter for ANSPs to determine what is acceptable in this regard for their implementation of STCA.

4.5 Context

It is essential, at the outset, that the ANSPs planning to implement STCA establish a clear STCA policy for their particular operational environment in order to avoid any ambiguity about its role and use. The adopted safety policy therefore sets part of the context for this argument. (**CONTEXT 01**).

The EUROCONTROL Specification for STCA has provided generic policy statements and these are adopted as the starting point for this argument:

“STCA is a safety net; its sole purpose is to enhance safety and its presence is ignored when calculating sector capacity”.

“STCA is designed, configured and used to make a significant positive contribution to the effectiveness of separation provision and collision avoidance”

The argument is developed taking account of the concept of operations and the associated requirements specified in the EUROCONTROL Specification (**CONTEXT 02**).

4.6 Assumptions

Any assumptions made at the outset about the system boundaries and operational environment should be stated in the argument (**ASSUMPTION 01**).

4.7 Strategy

The main strategy adopted in this argument is to show that if a correct STCA specification exists and is complied with both technically and operationally, the resulting system can be expected to meet Criteria 01 & 02. The argument and evidence to support this strategy is developed in the following Figures and paragraphs.

4.8 Arg 1 STCA functional & performance requirements are specified which if implemented can be expected to meet the primary safety objective for STCA & Cr 01.

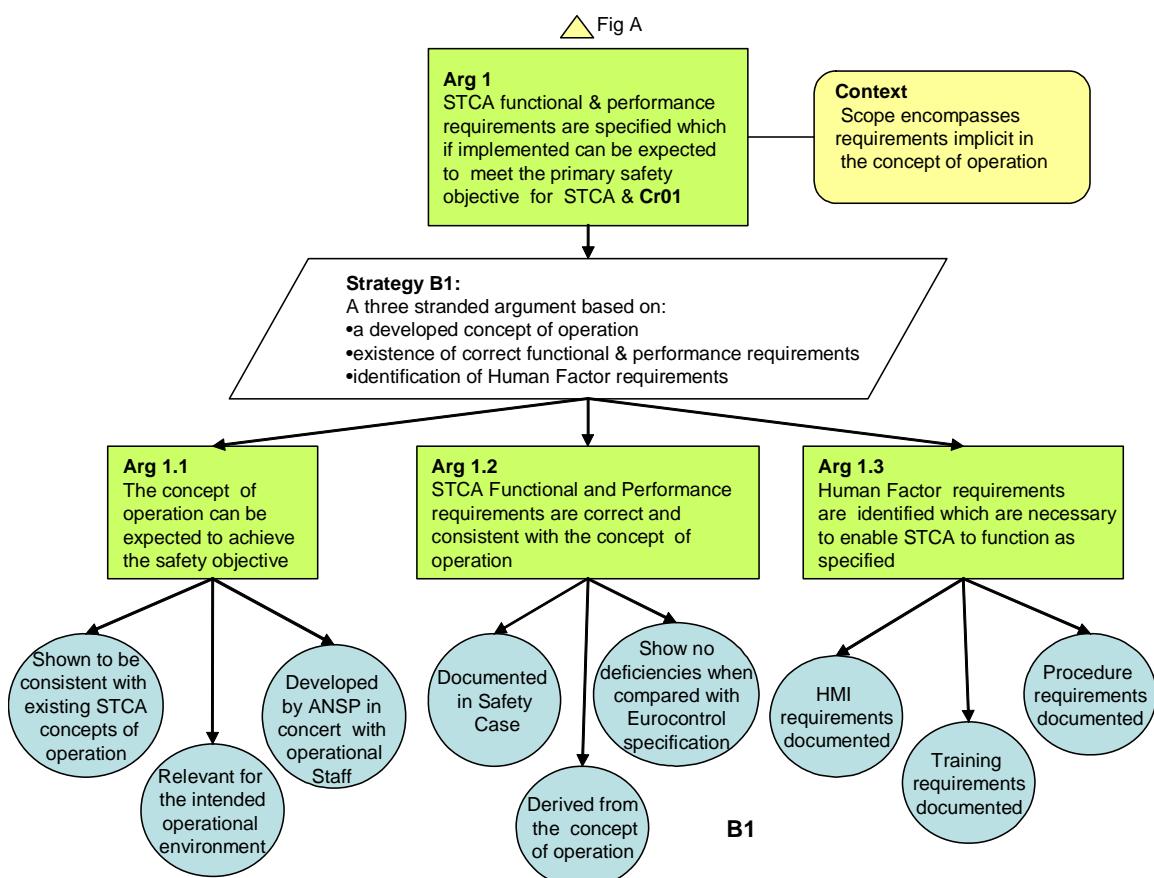


FIGURE B1 FUNCTIONAL & PERFORMANCE ASSURANCE ARGUMENT

This argument deals with the STCA “success” case - ie that STCA can be expected to deliver a substantive safety benefit in the absence of failure

The word “expected” is used here because additional requirements might be revealed during the later stages of system development.

The strategy is to develop a three-stranded argument based on:

- a developed concept of operation
- existence of a correct functional & performance requirements
- identification of Human Factor requirements

This argument is developed in Figure B1 above

ARG 1.1 Unless a the concept of operation has been determined and agreed by the ANSP it is unlikely that a complete and correct specification can be produced, or one that is compatible with the EUROCONTROL Specification. Note also that the context of use is as important as the intrinsic properties of the STCA system in determining whether Cr 01 is met.

ARG 1.2 ANSPs will specify the functional and performance requirements for STCA, appropriate to their concept of operation and operational environment. These also relate to how safe STCA needs to be in the absence of failure i.e. the “success” case. The specification must be documented (as only documented specifications exist!). It must also be verified to be complete and correct.

ARG 1.3 There is a range of Human factor issues that must be addressed from the outset if system is to meet safety objective. The requirements for human machine interface with the STCA system need to be determined. The training requirements for the operators of the system need to be determined the requirements and operating procedures must be developed. All these must be formally documented for use in the next phases of system development.

Details about the evidence required, and the criteria for success are set out in the Table 7.1 of the Safety Plan.

4.9

Arg 2 Safety requirements are specified which if implemented can be expected to mitigate against potential hazards and satisfy Cr02

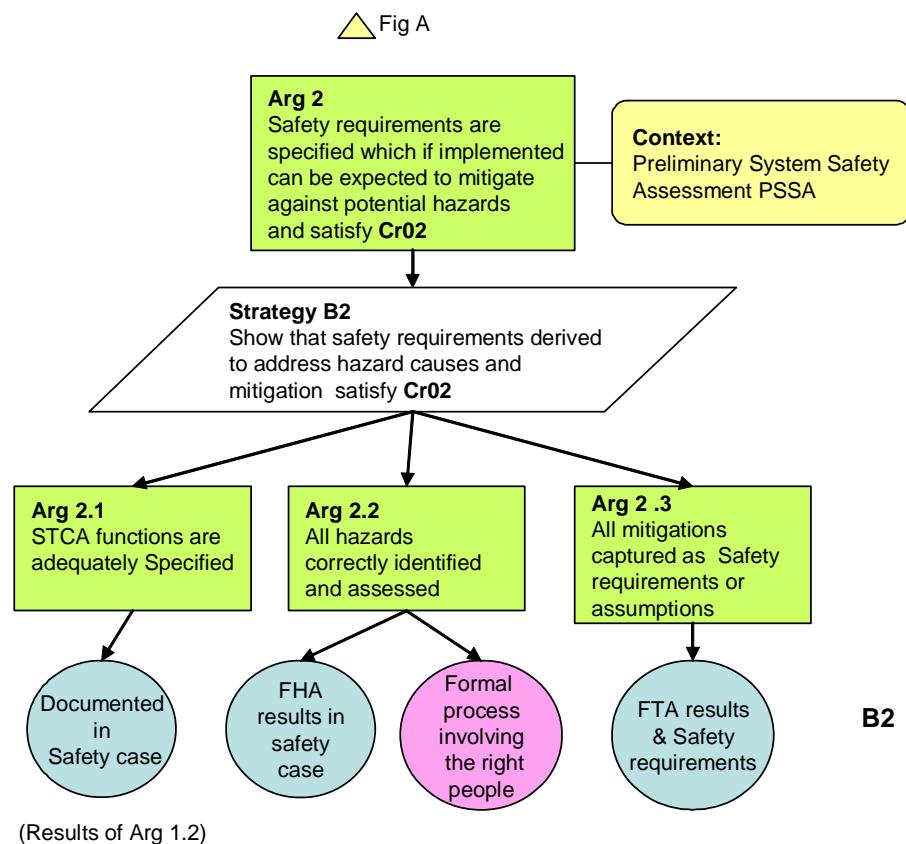


FIGURE B2 - SAFETY REQUIREMENTS ASSURANCE ARGUMENT

This argument deals with the STCA “failure case” i.e. how failures of STCA might have a negative safety impact on the rest of the ATM system. The Strategy here is to show that safety requirements derived to address hazard causes and mitigation can be expected to satisfy Cr02

This argument is developed in Figure B2 above.

ARG 2.1 The argument is dependent on evidence that the specification is consistent with the concept of operation. Additional assurance can be gained by showing that it is consistent with the EUROCONTROL specification for STCA.

ARG 2.2 Any increase in risk caused by failure of STCA should be small compared with the safety benefit to enable the benefit to be realised. To assess the risk it is necessary to identify the hazards, if any, which can result from functional failures of STCA. The process involves taking each of the specified functional requirements and subjecting them to a Functional Hazard Assessment FHA. The requirements for conducting an FHA are clearly set

out in the EUROCONTROL SAM. The results of the FHA are the primary source of safety requirements for hazard mitigation.

ARG 2.3 The Safety requirements are derived by taking each of the hazards identified and investigating how they might be caused. The causes will likely include some or all of the following:

- hardware and software failures,
- human error – errors of omission and commission by ATCOs and engineers
- procedure failures – errors in design or application.

Fault Tree Analysis (FTA) is one formal method for investigating the causes of hazards.

Details about the evidence required, and the criteria for success are set out in the Table 7.1 of the Safety Plan.

4.10 **Arg 3 The System Design correctly implements the functional, performance and safety Requirements**

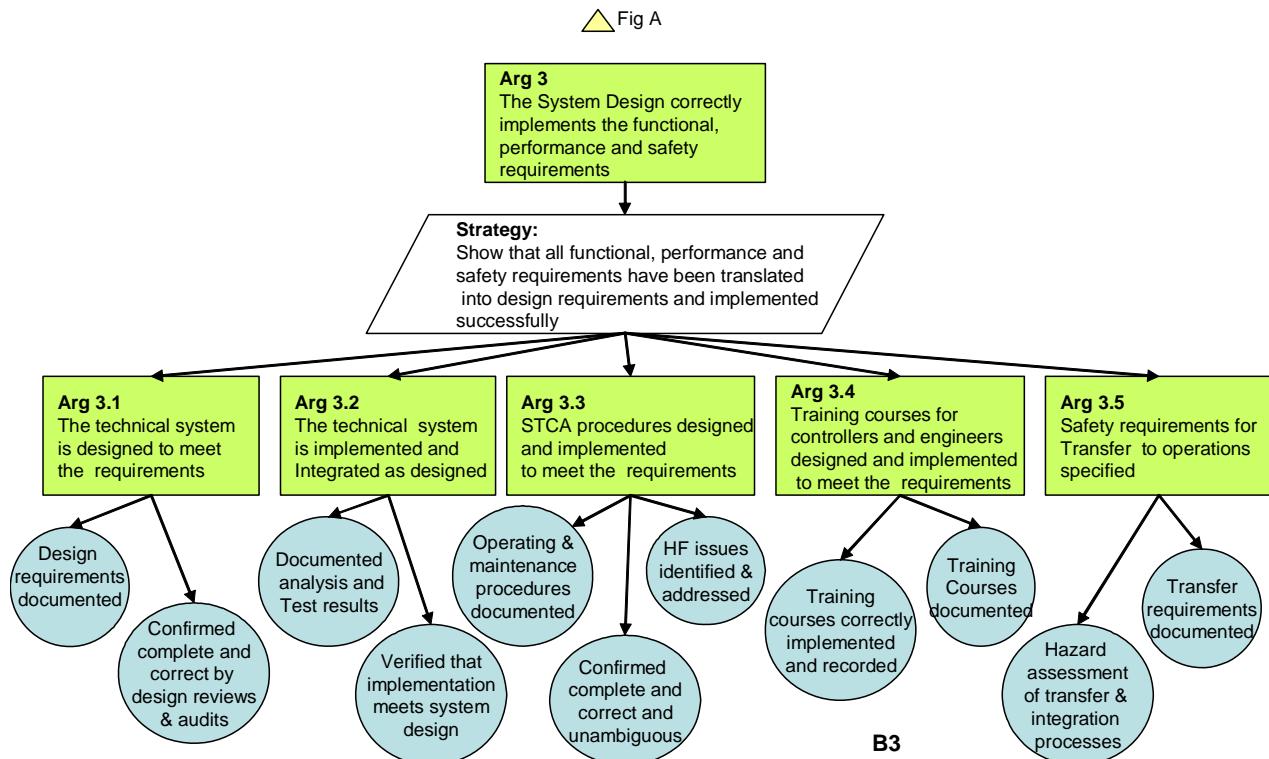


FIGURE B3 – SYSTEM DESIGN ASSURANCE ARGUMENT

The Strategy followed here is to show that all functional, performance and safety requirements have been translated into design requirements and implemented successfully.

ARG 3.1 It will be virtually impossible to show that the technical system is designed to meet the requirements if the design is not fully documented. The design can then be reviewed for completeness and correctness.

ARG 3.2 The technical system is implemented in hardware and software and integrated into the host ATC system as designed. The evidence for this will come from reviews, testing, analysis etc.

ARG 3.3 Procedures should be designed taking full cognisance of the operators point of view and related human factor issues, and with limited scope for ambiguity in understanding. Poorly designed ATC operational procedures and engineering maintenance procedures can be a contributory factor in incidents.

ARG 3.4 Controllers and Engineers should be trained and competent to operate the system and procedures.

ARG 3.5 The existing ATM system may be put at risk during the integration and transfer to operations of a new system - people, procedures and equipment included. It is important therefore that an assessment is made to identify any potential hazards that might need to be mitigated during that phase of activity.

Details about the evidence required, and the criteria for success are set out in the Tables 7.2 & 7.3 of the Safety Plan.

4.11 Arg 4 The risks associated with deploying the system have been reduced to a tolerable level

Two aspects of system deployment are addressed in this argument – transfer into operations and ongoing operation and maintenance.

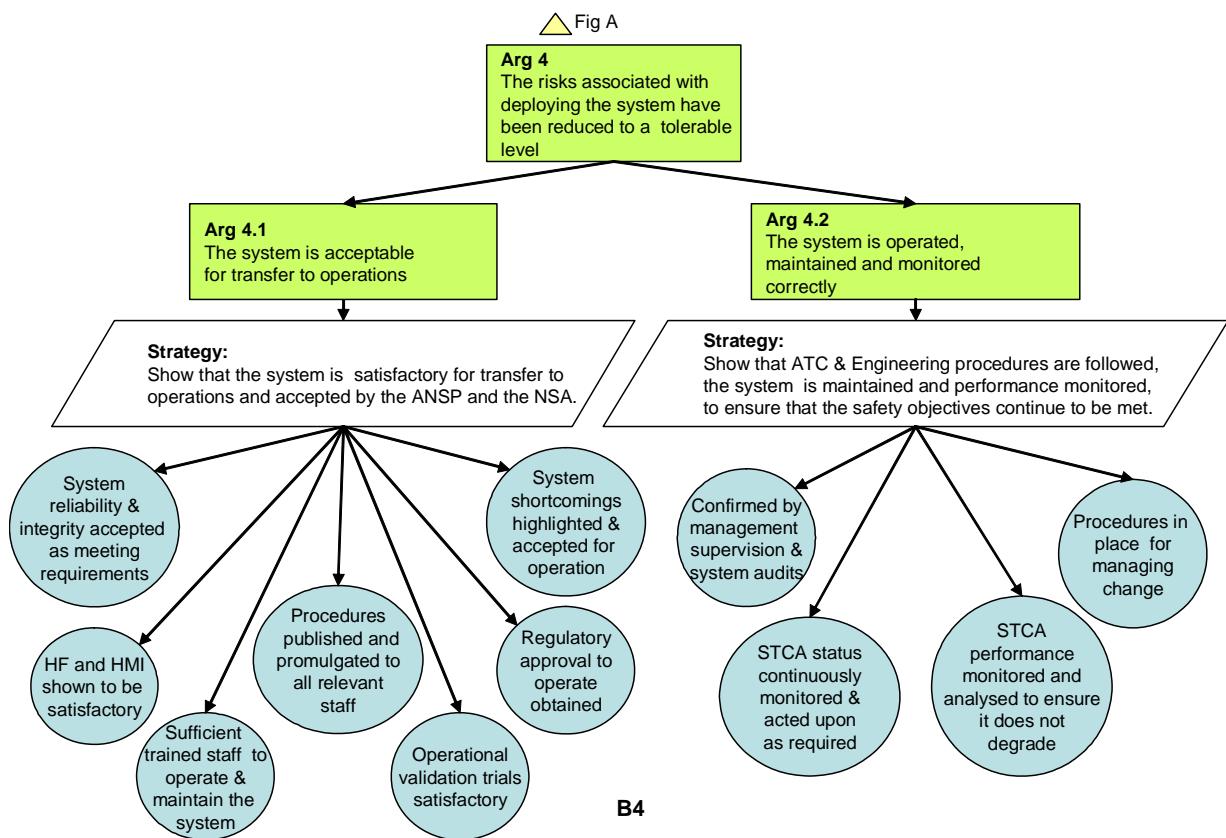


FIGURE B4 SYSTEM OPERATION & MAINTENANCE ASSURANCE

4.11.1 **Arg 4.1 The system is acceptable for transfer to operations**

The Strategy is to show that the system (people, procedures & equipment) is satisfactory for transfer to operations and accepted by the ANSP and the NSA. This is very much a decision for the ANSP. The ANSP will want assurance that the system is reliable; it should be at least as reliable as the host radar system in order to maximise the safety benefit. The ANSP will also want assurance that ATC is happy with it; that the necessary staff are trained and competent; that the regulator will approve it and that there are no outstanding issues that could impact on the safety of operations. Such assurance should be readily available in the safety case.

4.11.2 **Arg 4.2 The system is operated, maintained and monitored correctly**

The Strategy is to show that the operating & maintenance procedures are followed correctly, the system is maintained and its performance is monitored and to ensure that the safety objectives continue to be met.

STCA performance monitoring and analysis is a key issue in ensuring that STCA meets and continues to meet the criteria set down at the outset. Managers must ensure that the system remains optimised for its role and

keeps pace with ever changing operational requirements. They should also ensure that ATC behaviour in operating the system is consistent with ANSP STCA policy as well as not being compromised by system performance.

Details about the evidence required, and the criteria for success are set out in the Tables 7.4 and 7.5 of the Safety Plan.

END OF DOCUMENT