

EUROCONTROL



EUROCONTROL Guidance Material for Short Term Conflict Alert Appendix B-3: Outline Safety Case 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-3: Outline Safety Case for STCA System		
ALDA Reference:		06/12/14-23
Document Identifier	Edition Number:	1.0
	Edition Date:	14 December 2006
Abstract 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 outlines a possible Safety Case.		
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 ☐	General Public ☐	Intranet ☐
Draft ☐	EATM Stakeholders ☒	Extranet ☐
Proposed Issue ☐	Restricted Audience ☐	Internet (www.eurocontrol.int) ☒
Released Issue ☒	<i>Printed & electronic copies of the document can be obtained from ALDA (see page iii)</i>	

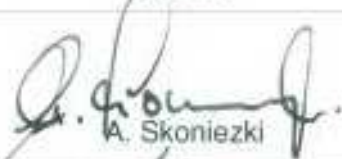
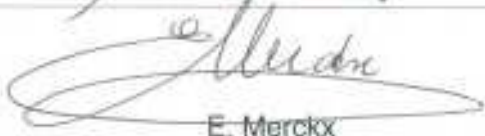
ELECTRONIC SOURCE		
Path:	\\HHBRUNA02\bakkerb\$\STCA	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	610 Kb

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. Skonieczki	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 Introduction	4
4.2 Safety Argument and Evidence Sections.....	5
4.3 Arg 0 Main Claim.....	5
4.4 Criteria 01 & 02	5
4.5 Context 01 Safety Policy for STCA	6
4.6 Context 02 Concept of Operation for STCA.....	7
4.6.1 ATC Control Loop.....	7
4.6.2 Operational Context	8
4.7 Assumption 01	9
4.8 Strategy A1	9
5. Functional and Performance Requirements	10
5.1 STCA functional and performance requirements are specified which if implemented can be expected to meet the safety criteria for STCA [Arg 1].....	10
5.2 Strategy	10
5.3 The concept of operation can be expected to achieve the safety objective [Arg 1.1].	11
5.4 STCA Functional and Performance requirements are correct and consistent with the concept of operation [Arg 1.2]	11
5.5 Human Factor requirements are identified which are necessary and sufficient to enable STCA to function as specified [Arg 1.3]	14
6. Safety Requirements.....	15

6.1	Safety Requirements are specified which if implemented can be expected to mitigate against potential hazards and satisfy Cr 02 [Arg 2]	15
6.2	STCA Functions are adequately specified [Arg 2.1]	16
6.3	All Hazard correctly identified and assessed [Arg 2.2]	16
6.3.1	Introduction.....	16
6.3.2	Scope of System Considered For FHA	16
6.3.3	Process.....	17
6.3.4	FHA Results	17
6.3.5	Safety Objectives and high level safety requirements	21
6.3.6	Safety requirements for hazard mitigation	21
6.4	All Causal Mitigations captured as Safety Requirements or assumptions [Arg 2.3].....	22
6.4.1	Introduction.....	22
6.4.2	System Architecture	22
6.4.3	Overall description.....	22
6.4.4	Alert Processor Description.....	23
6.4.5	ATCO role.....	23
6.4.6	Hazard Causes.....	23
6.4.7	FTA Boundary	23
6.5	System Level Safety Requirements.....	26
7.	Design Assurance	28
7.1	The system design correctly implements the functional, performance and safety requirements [Arg 3].....	28
7.2	Introduction	28
7.3	Strategy.....	28
7.4	The Technical System is designed to meet the Requirements [Arg 3.1].....	29
7.4.1	Overview of how the STCA system Works	29
7.4.2	Coarse Filter	30
7.4.3	Fine Filters.....	30
7.4.4	Linear Prediction (LP) filter.....	30
7.4.5	Current Proximity (CP) filter	31
7.4.6	Alert Confirmation.....	31
7.5	The Technical System is implemented and integrated as Designed [Arg 3.2]	31
7.5.1	Assurance for the implementation and integration.....	31

7.5.2	Summary of Assurance in the Design	32
7.6	STCA Procedures Designed and implemented to meet the requirements [Arg 3.3]	32
7.7	Training Courses for Controllers and Engineers designed and implemented to meet the requirements [Arg 3.4]	32
7.8	Safety Requirements for the Transfer to operations specified [Arg 3.5]	33
8.	System Transition, Operation & Maintenance	34
8.1	The risks associated with deploying the system have been reduced to a tolerable level (Arg 4)	34
8.2	Transfer to Operations	34
8.3	Operation and Maintenance	34
9.	Conclusions	35
9.1	Assumptions	35
9.2	Shortcomings	35
9.3	Limitations	35
9.4	Outstanding Safety Issues	35

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
- Generic Safety Plan for the implementation of STCA
- Outline Safety Case for STCA [This document]

The necessary safety assurance is obtained by following a planned safety assessment process appropriate to each stage of the system development lifecycle. This document follows the process as described in EUROCONTROL Safety Assessment Methodology (SAM). It addresses in detail the assurance and evidence from the System Definition stage within the SAM lifecycle. It outlines the likely assurance and evidence for the later stages.

Individual ANSPs implementing STCA might be starting from different points, and their concept of operations, requirements and designs may differ. Guidance is provided throughout this document where individual ANSPs may need to deviate from, the arguments and evidence in this outline safety case.

If ANSPs adopt a lifecycle different to one in SAM, they will need to revise this outline 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 an outline structure for a safety case that can be used by ANSPs in documenting safety assurance for STCA applications. A safety case for STCA should provide sufficient assurance to satisfy an ANSP and their National Safety Authority that the STCA system will meet, and continue to meet its safety objectives and safety requirements. The necessary safety assurance is obtained by following a planned safety assessment process appropriate to each stage of the system development lifecycle. This document follows the process described in EUROCONTROL Safety Assessment Methodology (SAM) and complies with the **essential** requirements of the EUROCONTROL Safety Case Development Manual (SCDM).

GUIDANCE: This document is the Outline Safety Case for STCA. Its purpose is to provide guidance material for ANSPs to assure their own implementations of STCA in accordance with the EUROCONTROL Specification. It addresses in detail the assurance and evidence from the System Definition stage within the SAM lifecycle. It outlines the likely assurance and evidence for the later stages.

Individual ANSPs implementing STCA might be starting from different points, and their concept of operations, requirements and designs may differ. Guidance is provided throughout this document where individual ANSPs may need to deviate from, or augment the arguments and evidence in this Outline Safety Case.

If ANSPs adopt a lifecycle different to one in SAM, they will need to revise this Outline Safety Case.

3. SCOPE

This Outline Safety Case contains details of the safety assurance necessary to support the claim that STCA will provide a substantive safety benefit in ATM operations. The argument supporting this claim is presented herein, along with the related evidence.

Only the assurance derived during system definition phase of the STCA lifecycle is covered in any detail. An outline is given of the safety assurance required from the other lifecycle phases. The assurance was derived in accordance with the Generic Safety Plan for the Implementation of STCA and each assurance item is linked by reference to the activities listed in the Safety Plan thus: [SP 7.1.1]

The Safety Case is derived from the overall argument structure described in the document, "Safety Argument for Short Term Conflict Alert", through activities described in the Generic Safety Plan for STCA Implementation. Whereas that document outlines the safety argument, this safety case implements that argument and provides the evidence to instantiate it.

GUIDANCE: STCA is a function provided within the surveillance system and intricately dependent on it. As such, ANSPs may legitimately decide not to have a stand alone safety case for STCA, but to include the assurance in the safety case for the surveillance system.

4. OVERALL SAFETY ARGUMENT

4.1 Introduction

The overall argument is structured as shown in Figure A below. The sub arguments are mapped onto 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 the safety case.

4.2 Safety Argument and Evidence Sections

These following sections present each of the strands of the safety arguments in turn, together with the supporting evidence to show that each of the claims is met.

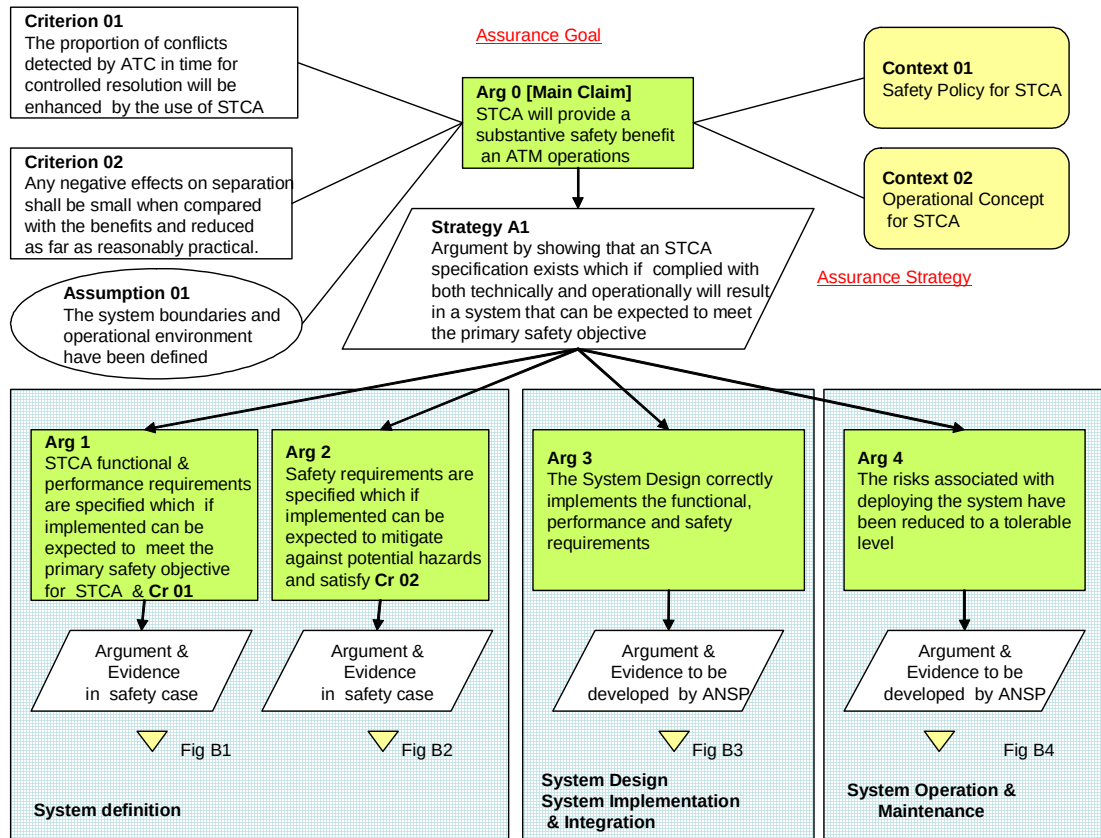


FIGURE A OVERALL ARGUMENT STRUCTURE

4.3 Arg 0 Main Claim

The main claim for which assurance is required is that “STCA will provide a substantive net safety benefit in ATM operations”.

4.4 Criteria 01 & 02

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

GUIDANCE: In a EUROCONTROL context, the word ‘substantive’ is taken to mean that a high percentage of conflicts eligible for STCA protection would be alerted to the Controller within an acceptable warning time.

Criteria for judging the safety benefits are:

- **CRITERION 01**, the proportion of conflicts detected by the Controller will be enhanced by the use of STCA – i.e. STCA will make a significant contribution to safety, and
- **CRITERION 02**, any negative effects on safety is small compared with the safety benefit.

GUIDANCE: Depending on ANSPs safety management arrangements and regulatory arrangement, it is possible that some ANSPs will wish to provide quantifications of these two criteria [SP 7.1.1]. The actual quantification is a matter of National Choice.

ANSPs who have already implemented STCA may be able to quantify the safety benefit based on historical performance data.

For some ANSPs, it is likely that a qualitative argument about the benefits will have to be made initially.

Illustrative Examples:

Example of a quantified system requirement derived from Criterion 1:

80% of eligible conflicts are to be alerted, of which 80% have a warning time of 30 seconds or more.

Example of a quantified system requirement derived from Criterion 2:

The number of nuisance alerts shall comprise less than 1% of all alerts displayed to the controller.

4.5 Context 01 Safety Policy for STCA

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.

GUIDANCE: One of the first tasks of an ANSP when deciding to implement an STCA system is to determine the **policy** regarding the use of STCA [Safety Plan 7.1.2]. It is essential that individual ANSPs establish a clear STCA policy for their particular operational context to avoid ambiguity about the role and use of STCA. This process is likely to coincide with the ANSP actions to determine the basic operational objectives for the system and the **concept of operations** [Safety Plan 7.1.3].

The EUROCONTROL Specification for STCA has provided generic policy statements to aid this process, and these are adopted as the starting point for this safety case:

“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 inference to be drawn from this policy is that the Controller's responsibility for maintaining safe separation is no different with or without STCA.

GUIDANCE: This Outline Safety Case is based on the EUROCONTROL Specification for STCA, and hence the policy it describes. If ANSPs adopt a different policy they will need to adapt the safety case accordingly.

An Illustrative STCA policy which differs from that stated in the EUROCONTROL Specification one:

ILLUSTRATIVE EXAMPLE: STCA is a safety net. Its purpose is to enhance safety by alerting controllers to potential conflicts, without impairing safety by distracting the controller unnecessarily.

It is important to recognise that STCA does not function as a separation assurance tool: it not necessary for there to be a loss of separation to generate an STCA alert; nor will STCA alert on every loss of separation.

4.6 Context 02 Concept of Operation for STCA

The Concept of Operation sets the **CONTEXT** for the safety case.

The concept of operations upon which this Outline Safety Case is based was developed by the SPIN Task Force, an expert group from EUROCONTROL and ANSPs, one of the tasks of which was to develop the EUROCONTROL Specification for STCA. This is described in the sections that follow.

GUIDANCE: ANSPs should develop their own concept of operation in concert with operational staff, and agree it with them. If the ANSPs concept of operation is different from the one provided here, that concept should be recorded in the safety case at this point together with the assurance that it is complete and correct and consistent with ANSP policy for STCA. [Safety Plan 7.1.3]

4.6.1 ATC Control Loop

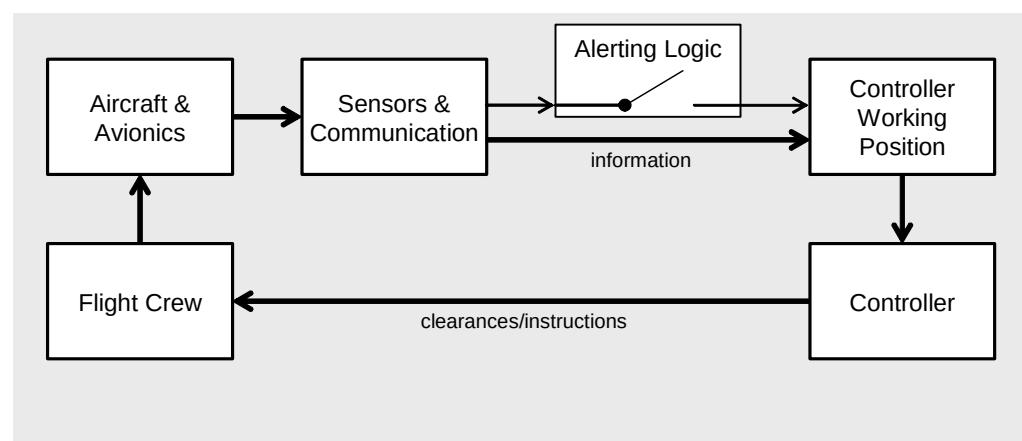


Fig. 1: Simplified ATC Control Loop

As illustrated in Fig. 1, today's ATC system is human centred: based on processing of a continuous stream of information, the controller issues clearances and instructions to prevent or resolve conflicts.

However, the drive for consistency in cognitive information-processing tasks leads to selective perception/exposure, selective attention and selective interpretation. As a result, conflicts and deviations from clearances or instructions leading to aircraft proximity can remain unnoticed.

STCA adds independent alerting logic to the control loop by generating indications of existing or pending situations, related to the proximity of aircraft as well as their relative positions and speed, which require attention/action.

STCA is intended to function in the short term, by providing warning times up to 2 minutes. The achieved warning time depends on the geometry of the situation. The maximum warning time may be constrained in order to keep the number of nuisance alerts below an acceptable threshold.

4.6.2 Operational Context

When STCA was first introduced in the mid nineteen-eighties, radar services were in most cases provided using mixed (raw radar data amplified with computer-generated synthetic data) situation displays. In the meantime, the norm for provision of radar services has become full-synthetic situation displays in most ECAC States. Decision support tools are gradually being introduced to enable the controller to handle more traffic in order to cope with the ever increasing demand. At the same time, automated system support has become more robust and trustworthy but also more complex and interdependent. These changes imply a different operational context for STCA.

STCA is only effective if the number of nuisance¹ alerts remains below an acceptable threshold according to local requirements and if it provides sufficient warning time to resolve hazardous situations, governed by the inherent characteristics of the human centred system.

¹ A Nuisance Alert is defined in EUROCONTROL Specification as an Alert which is correctly generated according to the rule set but is considered operationally inappropriate.

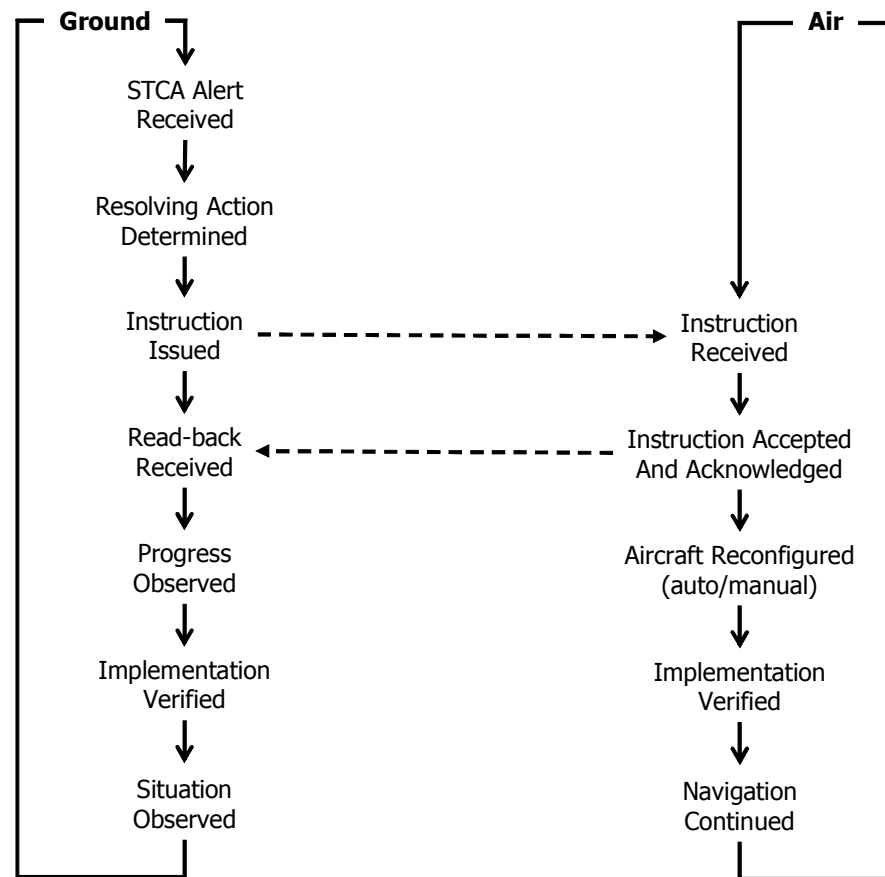


Fig. 2: Expanded ATC Control Loop (triggered by STCA)

Fig. 2 illustrates the nominal sequence of events to resolve a particular situation as two loosely coupled state charts. Being a human centred system, the Ground chart reflects the states of the controller and the Air chart reflects the states of the flight crew. For each state transition to occur certain preconditions have to be met and actions performed, complicated by many fixed or variable delays and anomalous cases.

4.7 Assumption 01

Any assumptions made at the outset about the system boundaries and operational environment should be stated here.

GUIDANCE: STCA may be integrated into the existing ATM system and may be operated in designated sectors and associated operational environment. The feasibility of any assumptions in this regard need to be verified at the outset and confirmed to be unchanged at implementation of the system. [SP 7.1.4]

4.8 Strategy A1

The main strategy adopted to meet the above claim 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.

This is dependent on satisfying four Arguments (Arg 1 to Arg 4) as represented in Goal-structuring Notation (GSN)² in Figures B1 to B4.

5. FUNCTIONAL AND PERFORMANCE REQUIREMENTS

5.1 STCA functional and performance requirements are specified which if implemented can be expected to meet the safety criteria for STCA [Arg 1].

This argument deals with the “success” case – i.e. 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 assurance required is outlined in Figure B1 below.

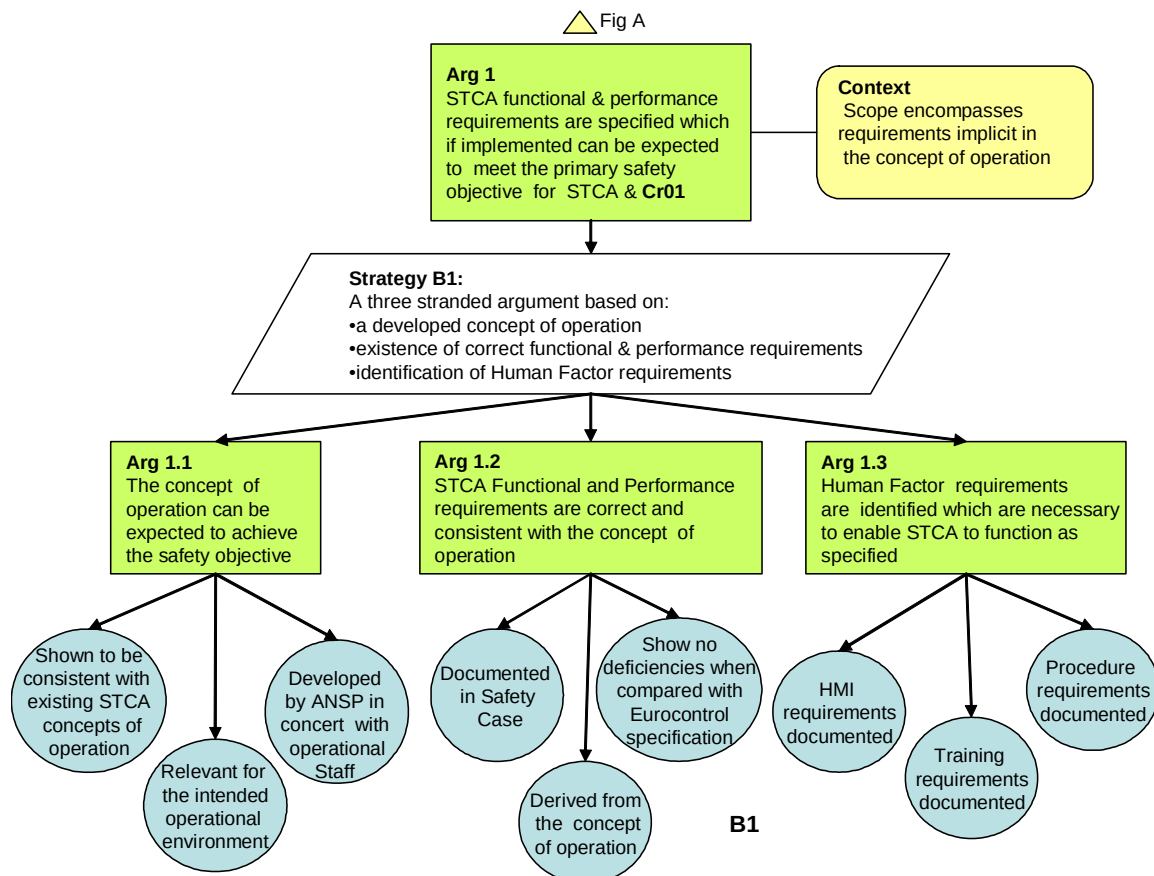


FIGURE B1 FUNCTIONAL & PERFORMANCE ASSURANCE ARGUMENT

5.2 Strategy

The strategy for assurance is based on satisfying the following sub claims:

- The existence of a developed concept of operation

² This is the adapted form recommended by the EUROCONTROL SCDM.

- the existence of a correct functional & performance requirements specification.
- Human Factor requirements are identified which are necessary to enable STCA to function as specified.

The available assurance is described in the following paragraphs.

5.3 **The concept of operation can be expected to achieve the safety objective [Arg 1.1].**

STCA is not a new concept, and has been implemented and operated satisfactorily by a number of ANSPs for many years.

The concept of operations contained in the EUROCONTROL Specification is consistent with that in use by ANSPs. Also, as the concept of operation from the EUROCONTROL Specification for STCA was developed by an expert group, which included ANSPs it is **CLAIMED** that it is consistent with ANSP's concept. [Safety Plan 7.1.3]

GUIDANCE: If an ANSP is currently using an STCA system, it will need to document here the evidence that it is consistent with the EUROCONTROL concept, or otherwise show that this claim is met.

If an ANSP is not currently using an STCA system and it is able to use the EUROCONTROL concept of operation then it can document that here and the claim will be met.

In either case, ANSPs should note that the operational environment e.g. volumes of airspace where STCA is to be operated is not elaborated in the concept of operation. This is a matter for ANSPs to address. [Safety Plan 7.1.4]

5.4 **STCA Functional and Performance requirements are correct and consistent with the concept of operation [Arg 1.2]**

The functional requirements extracted from the EUROCONTROL Specification are documented in the following Tables.

GUIDANCE: Assurance is required that implementing the specified functional & performance requirements can be expected to deliver the safety benefit. [SP 7.1.5]

ILLUSTRATIVE EXAMPLE:

Since the requirement is for a 30 second warning time, and since the STCA policy is to alert to conflicts, and since nuisance alerts must be minimised, the three part alerting criteria will ensure that urgent alerts are notified immediately and that nuisance alerts are minimised.

Since the confirmation and delay terms are configurable, these numbers can be refined in test and in operation to ensure that the criteria are optimally met.

It is **CLAIMED** that they show compliance with the requirements identified in the concept of operation.

GUIDANCE: The tables in the following sections provide a useful means of showing correctness and consistency with the concept of operations. If ANSPs concept of operations and/or functional and performance requirements are different from the EUROCONTROL ones, ANSPs will need to adapt the content of these tables to reflect their own information.

It is **CLAIMED** they show no deficiencies with the EUROCONTROL specification as they were extracted from it.

GUIDANCE: This Outline Safety Case uses the EUROCONTROL Specification as the definition of the functional requirements. By definition these are consistent with themselves! If ANSPs concept of operations and/or functional and performance requirements are different from the EUROCONTROL ones, ANSPs will need to add information here to show that their specification shows no deficiencies with respect to the EUROCONTROL Specification. Note that the EUROCONTROL Specification sets minimum requirements only and ANSP specifications are likely to be more specific, especially in relation to performance requirements. However, comparison of ANSP specifications with EUROCONTROL Specification can help to determine completeness of the former.

Req No:	Policy and Organisational Requirements
STCA-01	The ANSP shall have a formal policy on the use of STCA consistent with the operational concept and safety management system applied.
STCA-02	The ANSP shall assign to one or more staff, as appropriate, the responsibility for management of STCA

TABLE 5A

Concept of Operation:	
STCA adds independent alerting logic to the control loop by generating indications of existing or pending situations, related to the proximity of aircraft as well as their relative positions and speed, which require attention/action.	
Req No:	Functional Requirement
STCA-08	STCA shall detect and alert operationally relevant conflicts involving at least one eligible aircraft.
STCA-09	STCA shall provide the ATC HMI with alert data for operationally relevant conflicts.
STCA-10	STCA shall provide alerts that attract the controller's attention and identify the aircraft involved in the conflict; STCA alerts shall be at least visual.
STCA-14	STCA shall continue to provide alert(s) as long as the alert conditions exist.
STCA-16	Alert Inhibitions shall be made known to all the controllers concerned.
STCA-17	Status information shall be presented to supervisor and controller working positions in case STCA is not available.
STCA-18	All pertinent STCA data shall be made available for offline analysis.

TABLE 5B

Concept of Operation: STCA is intended to function in the short term (as the name implies), by providing warning times up to 2 minutes. STCA is only effective if the number of nuisance alerts remains below an acceptable threshold according to local requirements and if it provides sufficient warning time to resolve the situation, governed by the inherent characteristics of the human centred system.	
Req No:	Performance Requirement
STCA-11	The number of nuisance alerts produced by STCA shall be kept to an effective minimum.
STCA-12	The number of false ³ alerts produced by STCA shall be kept to an effective minimum.
STCA-13	When the geometry of the situation permits, the warning time shall be sufficient for all necessary steps to be taken from the controller recognising the alert to the aircraft successfully executing an appropriate manoeuvre.
STCA -07	STCA performance shall be analysed regularly.

TABLE 5C

GUIDANCE: ANSPs will need to have functional and performance requirements for STCA appropriate to their concept of operation and operational environment. This will inevitably be more detailed than the EUROCONTROL Specification.

ILLUSTRATIVE EXAMPLE:

Requirement: An STCA alert is to be sent to the controller work station:

- (a) Immediately, in the case where a potential conflict detected by any filter shows a risk of an imminent collision;
- (b) After a configurable number of cycles confirming the potential conflict, unless during those cycles case (a) applies.
- (c) After a configurable delay period where there is still time for a lateral or vertical manoeuvre, unless during that delay case (a) applies

Traces To: STCA-08; STCA-09; STCA-13

Requirement: An STCA Alert is to be displayed on the controller workstation with an associated severity value:

HIGH – [Defined Alert Conditions]

MEDIUM – [Defined Alert Conditions]

LOW – [Defined Alert Conditions]

³ A False Alert is defined in the Eurocontrol Specification as an Alert which does not correspond to a situation requiring particular attention or action (e.g. caused by split tracks and radar reflections).

Traces To: STCA-09; STCA-11; STCA-12

5.5 Human Factor requirements are identified which are necessary and sufficient to enable STCA to function as specified [Arg 1.3]

GUIDANCE: The HMI should be designed to assist the controller in immediately determining the aircraft involved, as well as the geometry and time – criticality of the situation.

Req No:	HMI Requirement
STCA-09	STCA shall provide the ATC HMI with alert data for all relevant conflicts. [Safety Plan 7.1.6]
STCA-10	STCA shall provide alerts that attract the controller's attention and identify the aircraft involved in the conflict; STCA alerts shall be at least visual.

TABLE 5D

Req No:	Training Requirement
STCA-03	The ANSP shall ensure that all controllers are given specific STCA training, relevant to the STCA system that the controller will use. [Safety Plan 7.1.7]

TABLE 5E

Req No:	Procedure Requirement Safety Plan 7.1.8 & 7.1.11
STCA-04 (paraphrased)	Local instructions concerning the use of STCA shall be specified.
STCA-05 (paraphrased)	In the event an alert is generated the controller shall without delay assess the situation and if necessary take action to ensure that the applicable separation minimum will not be infringed or will be restored.
STCA-06 (paraphrased)	Following an alert, controllers shall be required to complete an incident report only in the event that a separation minimum was infringed.
STCA -07	STCA performance shall be analysed regulatory.

TABLE 5F

6. SAFETY REQUIREMENTS

6.1 Safety Requirements are specified which if implemented can be expected to mitigate against potential hazards and satisfy Cr 02 [Arg 2]

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. The argument is developed in Figure B2 below.

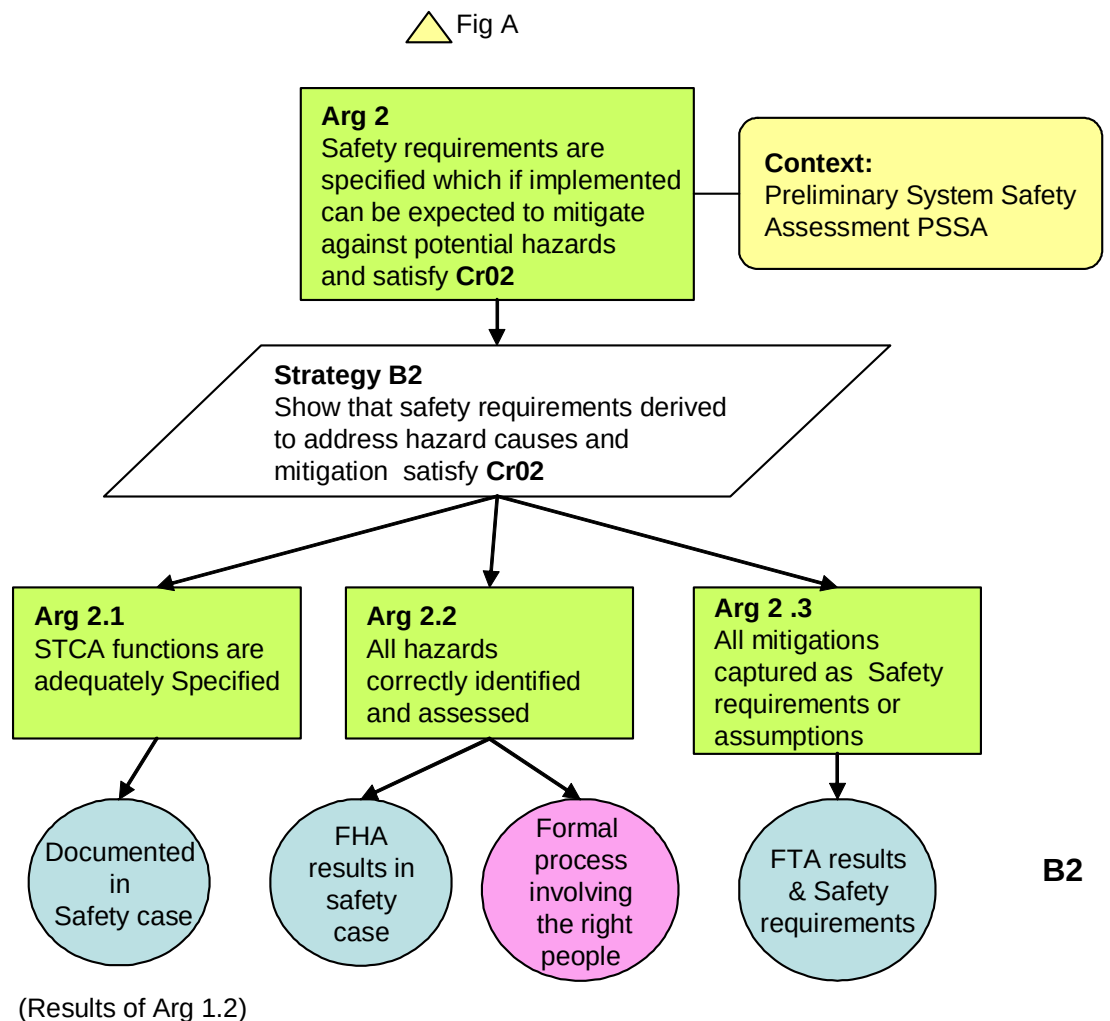


FIGURE B2 - SAFETY REQUIREMENTS ASSURANCE ARGUMENT

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) and Preliminary System Safety Assessment (PSSA). The FHA and PSSA processes followed were those defined in the EUROCONTROL SAM.

GUIDANCE: If ANSPs do not use the EUROCONTROL SAM process, they will need to document and justify the approach they do use.

6.2 STCA Functions are adequately specified [Arg 2.1]

The STCA functions are documented in the previous section.

GUIDANCE: The preliminary Safety Case has used the EUROCONTROL functions, if ANSPs do not use these they will need to refer to the appropriate set.

6.3 All Hazard correctly identified and assessed [Arg 2.2]

6.3.1 Introduction

The STCA functions specified in Section 5 were subjected to Functional Hazard Assessment (FHA) to determine how / when ATM conflict detection might not be enhanced by STCA and also to determine what negative effects (if any) STCA might have on separation provision and/or collision avoidance.

The FHA / PSSA addresses the 'failure case' for STCA, in which the consequences for the safety of ATM are explored by considering the effects on ATM operations resulting from loss, partial loss or corruption of the STCA functions. [Safety Plan 7.1.9]

The system boundaries include both civil and military airspace.

6.3.2 Scope of System Considered For FHA

When identifying hazards, different levels of hazards can be considered. A hazard is identified at the boundary of the scope of the system under assessment.

GUIDANCE: Some of the "hazards" associated with the 'failure case' (eg Table 6.1) might not be universally classified as hazards by the more traditional interpretation of the word - ie they will not cause or contribute to an accident, but they might reduce the chances of an accident being prevented. Nonetheless, treating them in this way provides for a uniform approach, and has no noticeable disadvantages.

For the purpose of this FHA, STCA is regarded as a safety net component of ATM and the assessment is scoped at this level. [Ref: EUROCONTROL SAM FHA Guidance Material].

The situation is illustrated in Figure 6.1 below. Three boundary levels were considered:

- ATM component level – treating STCA as a component.
- ATM level, where the effects of hazards will manifest themselves.
- Sub-system design level – source of hazards.

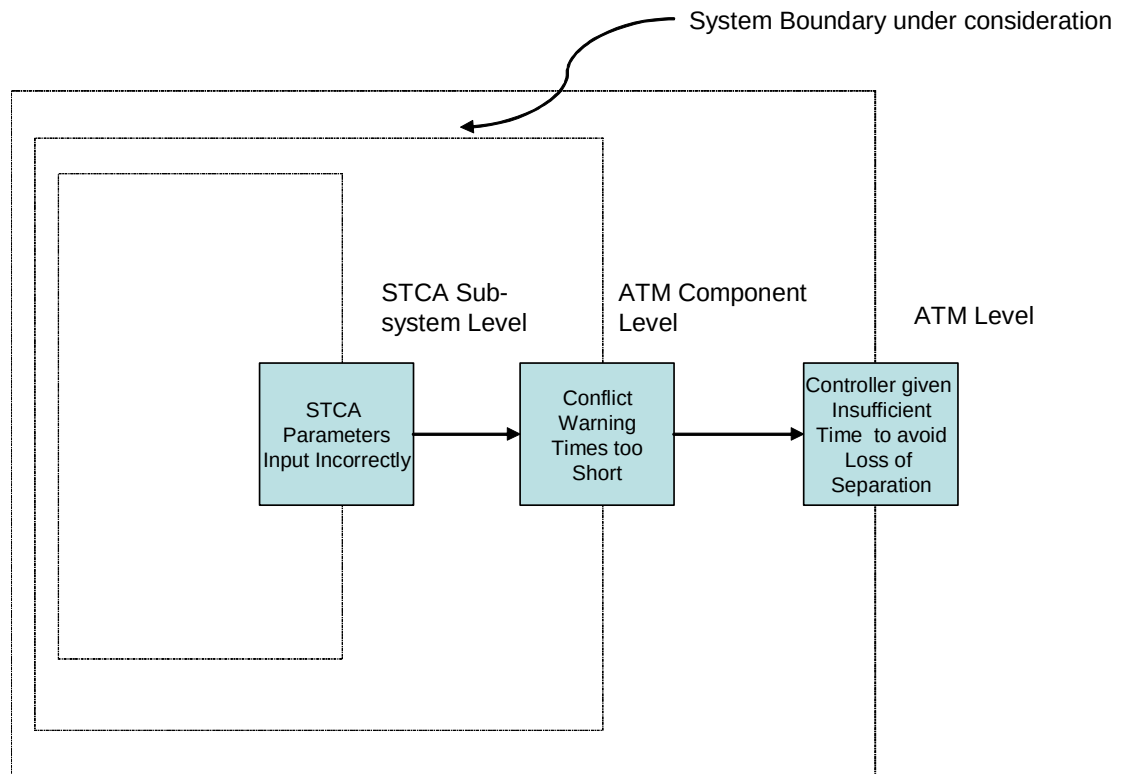


FIGURE 6.1 HAZARDS AT BOUNDARY OF SYSTEM UNDER ASSESSMENT

6.3.3 Process

The STCA functions specified in Section 5 were assessed during the FHA. The functional requirement reference number is included in the FHA Tables to provide traceability from the hazards to the functions.

GUIDANCE: It should be noted that the FHA results shown in the Tables below are based on the EUROCONTROL Specification for STCA, and are an example only. Inevitably ANSPs will need to refine these based on their own local circumstances, and two examples are included in the Tables. The results of the FHA will be expected to vary considerably with the operating environment, so the FHA should be carried out formally, by qualified ATC & Engineering staff by each ANSP. ATC input to this process is vital in order to ensure that the hazard effects are correctly stated and assigned the appropriate severity.

However, the results are consistent with the ANSP results in 6.3.4 below.

6.3.4 FHA Results

The FHA results are set out in the following Tables. The FHA is split into two parts: one (Table 6.1) dealing with hazards which undermine the 'success' case for STCA (i.e. reduces the risk-reduction effectiveness of the STCA functions) and the other (Table 6.2), dealing with hazards which introduce new risk.

Each of the hazards identified at the ATM Component boundary was assessed for effect on ATM. The severity of the effect was assessed using

the EATM SAM Severity classification scheme as a guide – FHA Guidance Material D. Safety Objectives have been expressed in relative terms; relative to the safety performance of ATM without STCA.

GUIDANCE: Safety Objectives normally govern the frequency of occurrence of hazards. Whether ANSPs have qualitative or quantitative measures of tolerable occurrence probabilities will depend on their own safety management processes and their regulatory requirements.

Loss of STCA merely undermines the success case (as should be the situation if STCA is not a capacity enhancer), and availability (rather than reliability) should be the determining parameter. ANSPs may decide to set a nominal target probability for this hazard taking into account the improvement in conflict detection attributable to their STCA. Thus, if STCA was expected to result in a net increase in the number of conflicts detected of 100 per sector, per year it might be decided that loss of automatic alerts up to 10 times per year, per sector will not impact significantly on the safety benefit. [See Example 6.1 in FTA Table 6.1].

An alternative approach might be to assume a simple linear relationship between net risk reduction attributable to STCA and STCA availability. It would be reasonable to assume that 90% availability would still constitute a significant safety benefit.

The effects of hazards resulting from the failure case may be quantifiable in the context of a typical risk classification scheme. See example 6.2 in FTA Table 6.2.]

EUROCONTROL Guidance Material for Short Term Conflict Alert
Appendix B-3: Outline Safety Case for STCA System

Hazard Ref: [Req. Ref]	Hazard – Defined at ATM Component Level	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation or ATS System factors	Safety Objectives
CA 1 [STCA-08] [STCA-09] [STCA-10] [STCA-14]]	Detected Total failure of STCA such that the Controller will not receive ANY automatic conflict Alerts	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts and there may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 4 Resolution and/or recovery functions slightly impaired for all relevant airspace for the duration of the loss of STCA. Possible slight increase in workload or stress, particularly at peak traffic times.	The Controller being aware of loss of STCA will be on heightened Alert. Radar tracks representation extended to highlight potential conflicts? Need to reinforce with a procedure for the provision of temporary alternative(s) to STCA	To reduce the number of total failures of STCA to a level and duration that will enable a significant safety benefit to be realised.
Illustrative Example 6.1	Loss of alert data at a sector suite.	Controllers are still able to maintain control despite there being a lowering of risk margins.	Loss of STCA is set to hazard severity category 4.		Loss of alert data at a sector suite shall have a target probability of occurrence of Probable. [In this scheme, Probable corresponds to probability of occurrence of up to 10 per year per sector of operations].
CA2 [STCA-10]	Controller attention not drawn to the automatic Alert	ATM safety not enhanced by STCA The Controller remains unaware of a potential conflict or may become aware too late to resolve it before a collision scenario develops	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	HMI for Alerting mechanism validated by controllers in operational environment	To ensure that no alerts are lost to the controller by reason of omissions or ergonomics as far as reasonably practical
CA3 [STCA-08] [STCA-09] [STCA-10] [STCA-14]]	Undetected partial loss of STCA functionality e.g. eligible volumes of airspace omitted inadvertently	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts and there may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Although undetected initially, the Controller is likely to detect the loss of functionality fairly quickly by observing the performance of STCA in situations where it would be expected to give an alert.	To reduce the number of occurrences of partial loss of STCA to a level and duration that will enable a significant safety benefit to be realised.
CA4 [STCA-13]	Automatic conflict warning times too short	ATM safety not enhanced by STCA The Controller may not receive timely warning of a potential conflict and it may have to be recovered by the pilot(s) or Controller emergency avoiding action.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	The Controller will be alert to situations and aircraft manoeuvres where STCA will not be able to give early warning	To ensure that conflict warnings are optimised in all relevant airspace as far as reasonably practical.
CA5	The Controller does not have a positive attitude to STCA	ATM safety not enhanced by STCA The Controller may not feel confident when operating at sector capacity thereby increasing risk of contributing to a loss of separation incident.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Comprehensive Training and clear STCA policy	To ensure that Controller's are adequately trained and competent so that the safety benefits of STCA can be realised operationally.

TABLE 6.1 STCA FHA – SAFETY NOT ENHANCED

EUROCONTROL Guidance Material for Short Term Conflict Alert
Appendix B-3: Outline Safety Case for STCA System

Hazard Ref: [Req. Ref]	Hazard – Defined at ATM Component Level	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation or ATS System factors	Safety Objectives
CA6 [STCA-11] [STCa-12]	Numerous Nuisance Alerts and possible False Alerts (credible corruption)	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to higher than non STCA levels.	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	If the number of nuisance Alerts is deemed unworkable the Controller will switch off the STCA function	To ensure that the number of nuisance alerts is reduced as far as reasonably practical.
Illustrative Example 6.2	Undetected corruption of alert data at a workstation in a sector suite.	May lead to increased Controller workload if the failure is such that excessive numbers of false alerts are issued.	Corruption of alerts is set to Severity 3		Undetected corruption of alert data at a workstation in a sector suite shall have a target probability of occurrence of Remote. [In this scheme, Remote corresponds to probability of occurrence of 1: 10 years per sector .
CA7 [ANSP Policy]	STCA used outside its scope as a safety net (i.e. as capacity enabler)	Negative effects on ATM Safety Traffic overload may occur when STCA fails thereby increasing the risk of conflicts developing	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedures in place to enforce safety net policy	To ensure that STCA is not used as a capacity enabler when it is specified as a safety net only.
CA8	No mitigation put in place in the event of STCA failures	Negative effect on ATM Safety Traffic overload may occur when STCA fails thereby increasing the risk of conflicts developing (failure to mitigate the consequences of CA 1 could constitute a hazard even when STCA is used strictly as a safety net)	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Where STCA is used purely as safety net no mitigation should be required in the event of failure. However, it may be prudent to some mitigation put in place if the traffic situation warrants it in the absence of STCA	To ensure that mitigation is put in place if the traffic situation warrants it in the absence of STCA

TABLE 6.2 STCA FHA - NEGATIVE EFFECTS ON ATM SAFETY

6.3.5 Safety Objectives and high level safety requirements

The Safety Objectives derived from the FHA are summarised in the Table 6.3 below. These will be decomposed to component-level safety requirements during the design phase PSSA. Each Safety Objective is given a unique identifier and a reference to the hazard to be mitigated.

GUIDANCE: The Safety Objectives developed by an ANSP will depend on their own FHA results. The Safety Objectives provided in the tables below will need to be adapted by ANSPs to reflect their own analysis. This may include quantifying these objectives.

SO Ref (Hazard Ref:)	STCA Safety Objectives & High Level Safety Requirements
SO 1 (Haz. CA 1)	The number of total failures of STCA shall be reduced to a level and duration that will enable a significant safety benefit to be realised. E.g. The number of total failures of STCA shall be less than 10 per year per sector at an ATS unit.
SO 2 (Haz. CA 2)	No alerts shall be lost to the controller by reason of omissions or ergonomics as far as reasonably practical
SO 3 (Haz. CA 3)	The number of occurrences of partial loss of STCA shall be reduced to a level and duration that will enable a significant safety benefit to be realised. E.g. The number of occurrences of partial loss of STCA shall be less than 10 per year per sector at an ATS unit.
SO 4 (Haz. CA 4)	Conflict warning times shall be optimised in all relevant airspace as far as reasonably practical.
SO 6 (Haz. CA 6)	The number of nuisance alerts shall be reduced as far as reasonably practical.

TABLE 6.3 SAFETY OBJECTIVES

6.3.6 Safety requirements for hazard mitigation

Additional safety requirements arise from FHA as follows (ref Fig 6.1 & 6.2):

SO Ref (Hazard Ref:)	Safety requirements for hazard mitigation
SRHM 1 (Haz. CA 2)	The HMI for the Alerting mechanism shall be validated by controllers in the operational environment.
SRHM 2 (Haz. CA 5)	Controller's shall be adequately trained and competent so that the safety benefits of STCA can be realised operationally.
SRHM 3 (Haz. CA 5)	Every effort shall be made (e.g. through having a clear policy, and comprehensive training) to ensure that Controllers have a positive attitude to STCA
SRHM 4 (Haz. CA 7)	STCA shall not used as a capacity enabler when it is specified as a safety net only.
SRHM 5 (Haz. CA 7)	Procedures shall be in place to enforce safety net policy.
SRHM 6 (Haz. CA 8)	Mitigation shall be put in place if the traffic situation warrants it in the absence of STCA

TABLE 6.4 SAFETY REQUIREMENTS

6.4 All Causal Mitigations captured as Safety Requirements or assumptions [Arg 2.3]

6.4.1 Introduction

The potential causes of the hazards identified during the FHA are investigated in this section. Safety requirements are set to mitigate the likelihood of the causes occurring. [Safety Plan 7.1.7]

This activity corresponds to the PSSA process described in SAM. Essential pre-requisite for conducting a PSSA are a description of the logical model of the system, including the system architecture; the human roles in the system; a description of the high-level functions of the system and their associated safety objectives and a list of hazards.

GUIDANCE: Some of these pre-requisites have been described previously in this Outline Safety Case, and may vary from those which ANSPs have established for themselves. The system architecture is described below in Figure 6.2.

The list of hazards and safety objectives comes primarily from FHA and is further completed during the PSSA.

6.4.2 System Architecture

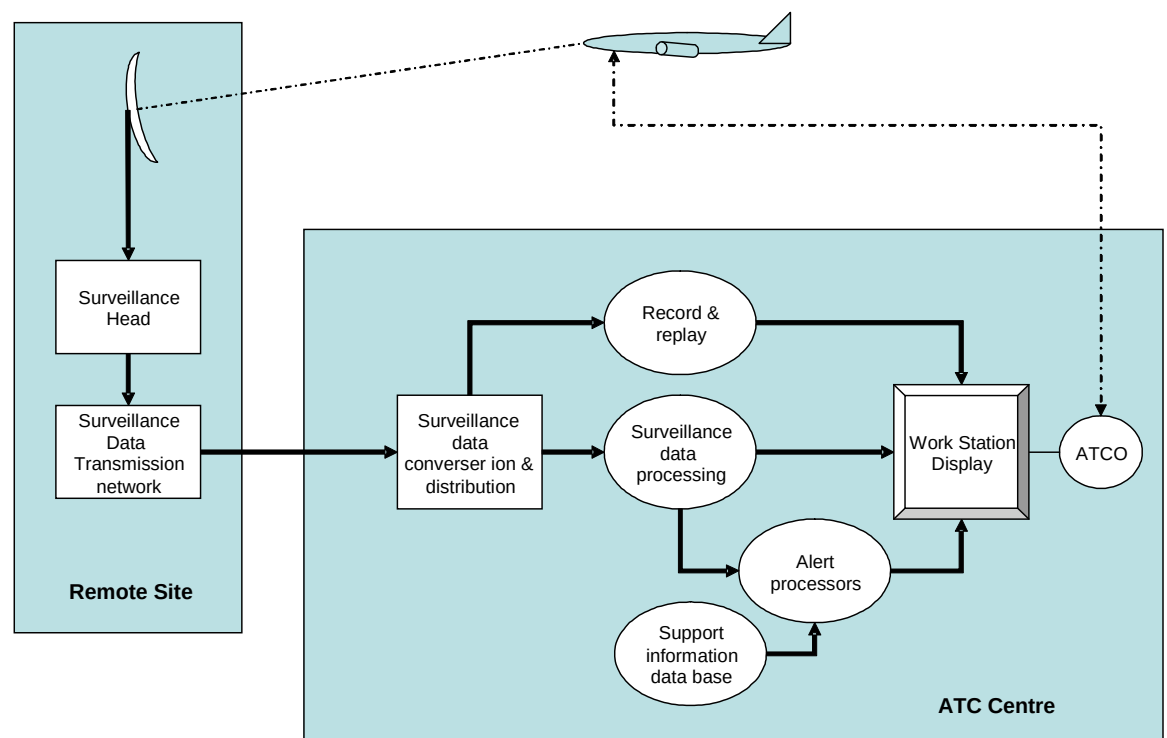


FIGURE 6.2- SYSTEM ARCHITECTURE

6.4.3 Overall description

The system comprises a typical multi-track radar system in which aircraft transponders upon interrogation by the ground radar transmitter reply with the

aircraft identity and position data. The data is transmitted from the remote site to the ATC Centre where it is processed and sent to the ATC workstation for display. The data is also recorded for later replay if necessary. The STCA function is hosted by the radar system in the Alert processor, supported by an information data base. Note: for the purpose of this safety case only those parts of the system within the ANSP scope to supply are included i.e. the aircraft systems are not included.

6.4.4 Alert Processor Description

The Short Term Conflict Alert (STCA) function monitors the multi-radar tracks in the area of interest and projects them ahead to check them for potential lateral and vertical positional conflicts. The Alert Processors process the multi-radar track data to generate Short Term Conflict Alerts. The Alert Processing computers only host the Short Term Conflict Alert function.

6.4.5 ATCO role

The role of the ATCO in responding to alerts is described earlier in the concept of operation.

6.4.6 Hazard Causes

The hazard causes were identified with the aid of Fault Tree analysis and the results are shown on Figures 6.2 and 6.3. Two top events were selected – one to explore the causes of the hazards that would result in ATM safety not being enhanced by STCA as much as it otherwise would be, and the other to explore the causes of hazards having a negative effect on separation provision or collision avoidance – i.e. introduce new risks.

GUIDANCE: ANSPs will need to establish for themselves the possible hazard causes, however, it is probable that because this Outline Safety Case has used an appropriately-generic logical architecture for an STCA system, that Figures 6.2 and 6.3 are re-usable.

6.4.7 FTA Boundary

The FTA causes are identified at STCA **system level** (refer to Figure 6.1) although some are identified at STCA component level to provide an insight into specific areas for which assurance evidence will be required. The hazard identifier e.g. CA1 is included.

GUIDANCE: The conventional way of showing fault trees is top down, and formal software tools are available for this purpose. In the examples which follow the fault trees are shown lying horizontally. This approach is useful when the output of fault trees is to be connected to event trees in order to investigate the consequences of the top event (the so-called bow-tie model). It is also more compact in applications such as this.

It should also be noted that there is no redundancy shown in these fault trees – i.e. all the branches are logical OR, not AND. That is not to imply that redundancy will not be necessary at component level. For example, dual processors may be required for both radar and alert processing for reliability purposes.

Although not fully developed here, particularly at component level, the fault trees for STCA should not need to be much bigger in practice. At most, one more layer at sub component level might be required when developing lower level requirements. E.g. the events that could result in STCA performance not being optimised could be included and translated into requirements.

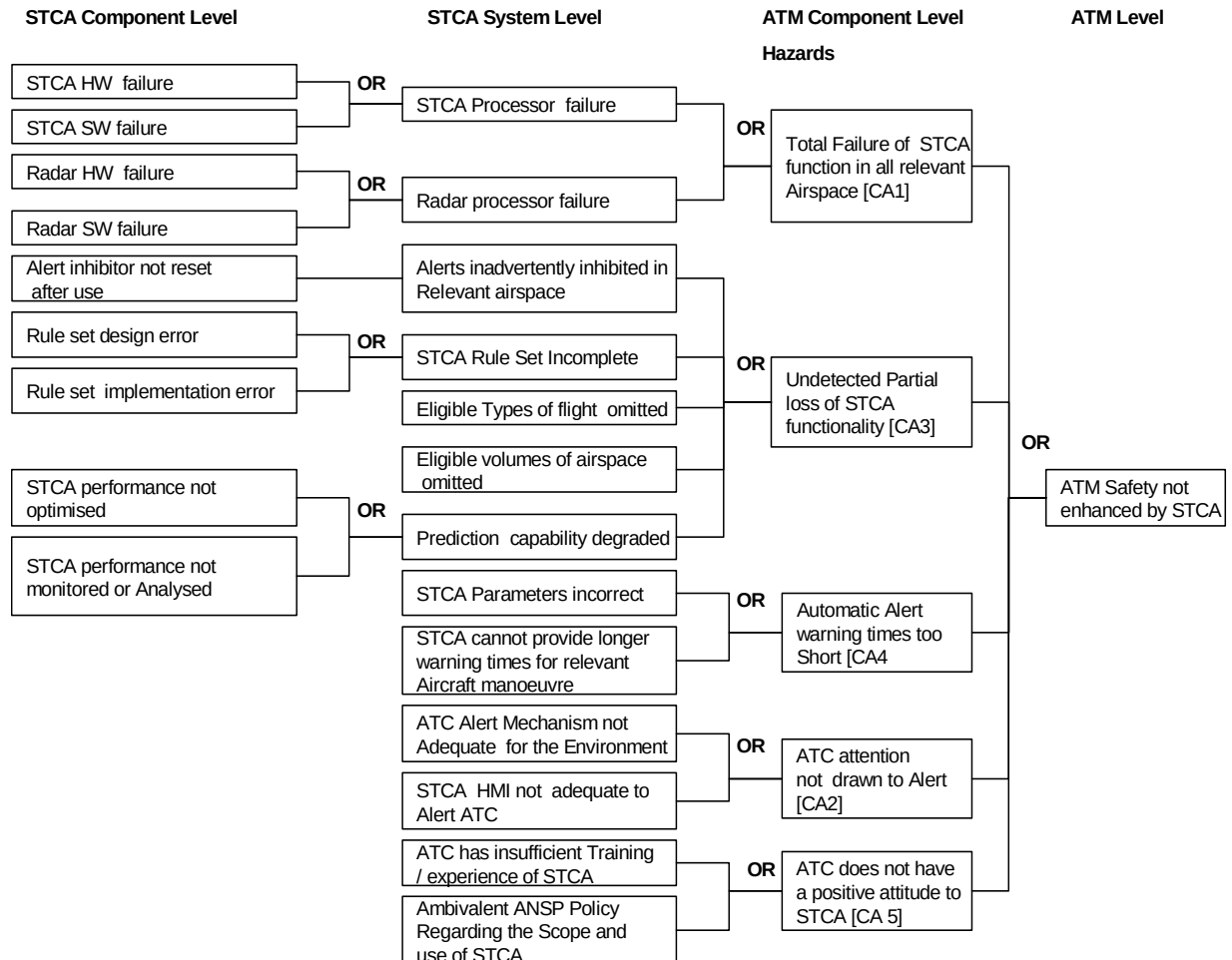


FIGURE 6.2 FAULT TREE FOR ATC CONFLICT RESOLUTION NOT ENHANCED BY STCA

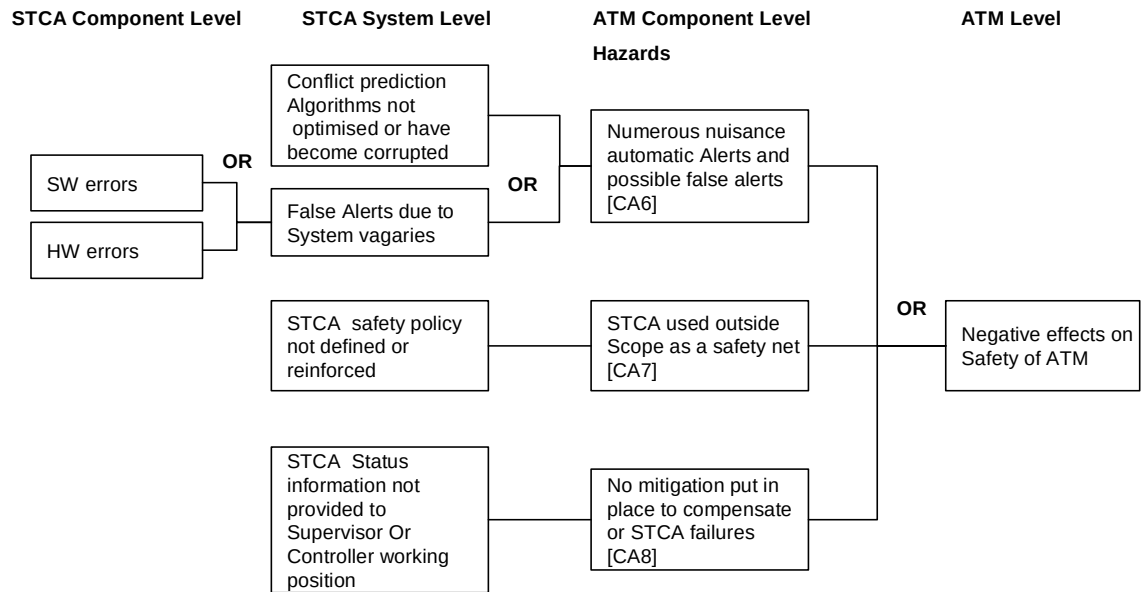


FIGURE 6.3 FAULT TREE FOR NEGATIVE EFFECTS ON ATM

6.5 System Level Safety Requirements

System Level Safety Requirements are derived from the Fault Trees so that the Safety Objectives will be met. These are included in the tables below.

GUIDANCE: The safety requirements shown in the tables below are derived from the EUROCONTROL specification, and the hazard analysis carried out above. ANSPs are likely to have to change the Safety Requirements stated below based on their own specifications and hazard analysis results.

Furthermore the requirements are purely qualitative. If ANSPs have safety management processes and/or regulatory requirements to quantify safety requirements, appropriate methods will need to be employed to do this, and the requirements below will need to be changed.

Ref No: (Hazard Ref:)	Technical System Safety Requirements
SRSL 1 (Haz. CA 1) (Haz CA 3)	The Technical system reliability should be to good commercial standard, preferably equivalent to that for the radar processor and exceeding that for the safety objectives SO 1 and SO 3 (<10 total failures per year)
SRSL 2 (Haz. CA 2)	The HMI for the automatic Alerting mechanism shall be capable of Alerting controllers in the operational environment
SRSL 3 (Haz. CA 8)	STCA status information shall be provided to Supervisor and to Controller working position
SRSL 4 (Haz. CA 3)	It shall be ensured that conflict prediction algorithms remain optimised and do not become corrupted.
SRSL 5 (Haz. CA 3)	It shall be ensured that parameters are validated for the relevant airspace and that they are installed correctly
SRSL 6 (Haz. CA 3)	It shall be ensured that the Rule sets etc are validated for completeness and correctness in the relevant airspace and they are installed correctly.
SRSL 7 (Haz. CA 3)	It shall be ensured that Alert inhibition process does not compromise the STCA function

TABLE 6 A

Ref No: (Hazard Ref:)	Procedure Safety Requirements
SRSL 8 (Haz. CA 2)	ATC procedures shall state what Controllers should do in the event of loss of an automatic alerting facility such as STCA.
SRSL 9 (Haz. CA 6)	The action to be taken when the number of nuisance Alerts is deemed to be excessive shall be addressed in local instructions/regulations.
SRSL 10 (Haz. CA 3)	Procedures shall be put in place to ensure that the Controller is advised of any system changes which might degrade the performance of STCA
SRSL 11 (Haz. CA 7)	STCA shall not used as a capacity enabler when it is specified as a safety net only.

TABLE 6 B

Ref No: (Hazard Ref:)	People Safety Requirements
SRSL 8 (Haz. CA 5)	Controllers shall be adequately trained and competent so that the safety benefits of STCA can be realised operationally.

TABLE 6 C

Ref No: (Hazard Ref:)	Management Safety Requirements
SRSL 8 (Haz. CA 5)	Clear and unambiguous policy shall be propagated to all ATC staff regarding use of STCA

TABLE 6 D

7. DESIGN ASSURANCE

7.1 The system design correctly implements the functional, performance and safety requirements [Arg 3]

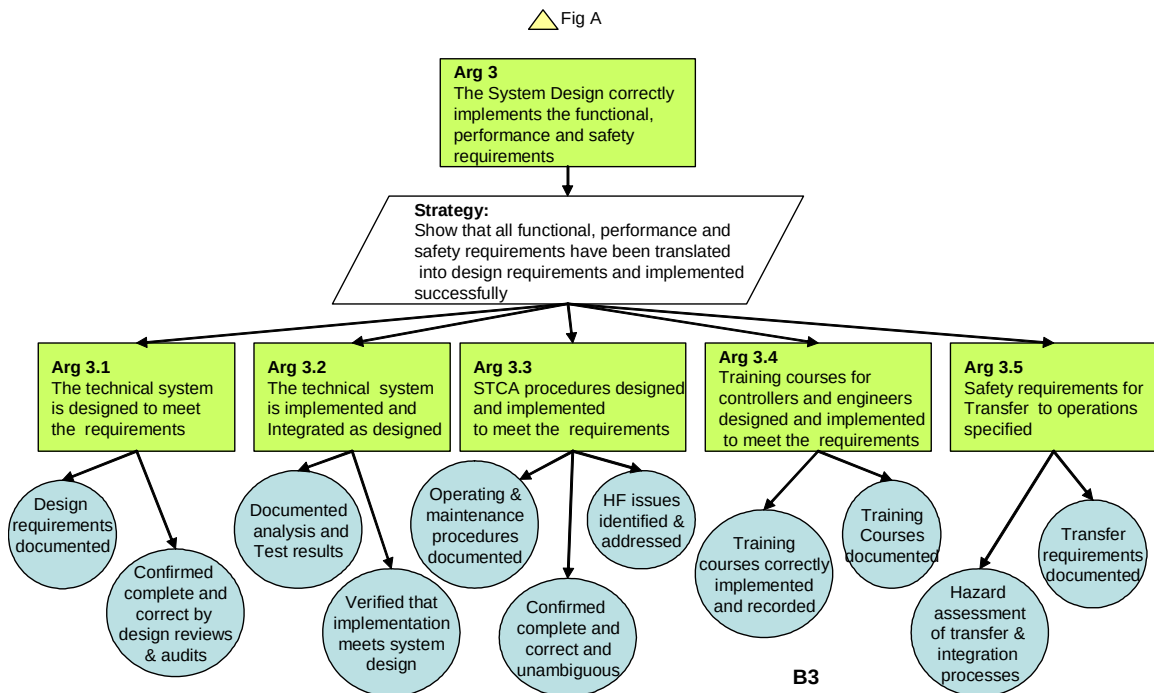


FIGURE B3 – SYSTEM DESIGN ASSURANCE ARGUMENT

7.2 Introduction

Assurance is required that the system design correctly implements the functional, performance and safety requirements relating to equipment, people and procedures.

7.3 Strategy

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

GUIDANCE: Design Assurance is beyond the strict scope of this Outline Safety Case, however it is possible to provide an overview of the approach and guidance to ANSPs on what design assurance might look like here and by reference to the Generic Safety Plan.

Actual design assurance will depend entirely on the actual architecture and design adopted by each ANSP.

7.4 The Technical System is designed to meet the Requirements [Arg 3.1]

GUIDANCE: A documented design is required, which is under configuration control and shown to be complete and correct. It will show how the functional requirements have been incorporated. It will outline how STCA works e.g. see below. It will contain detail descriptions (or references to documents containing these) of the STCA algorithms and filters etc. [Safety Plan 7.2.1 & 7.2.2]

7.4.1 Overview of how the STCA system Works

STCA utilises radar track data in order to alert controllers of possible conflicts between pairs of aircraft. There are a number of stages involved in processing the radar data, and each stage carries out a number of tests to see if the conflict should be passed to the next stage.

The system parameters used in these tests are designed to ensure an optimal balance between increasing wanted alerts and reducing nuisance alerts.

In order to account for differing traffic and separation standards, STCA divides airspace into regions, each of which can be allocated a different set of parameter values if required.

The following is a high level overview of how STCA works and some of the key parameters used, and as such is not intended to give a detailed account of the workings of STCA.

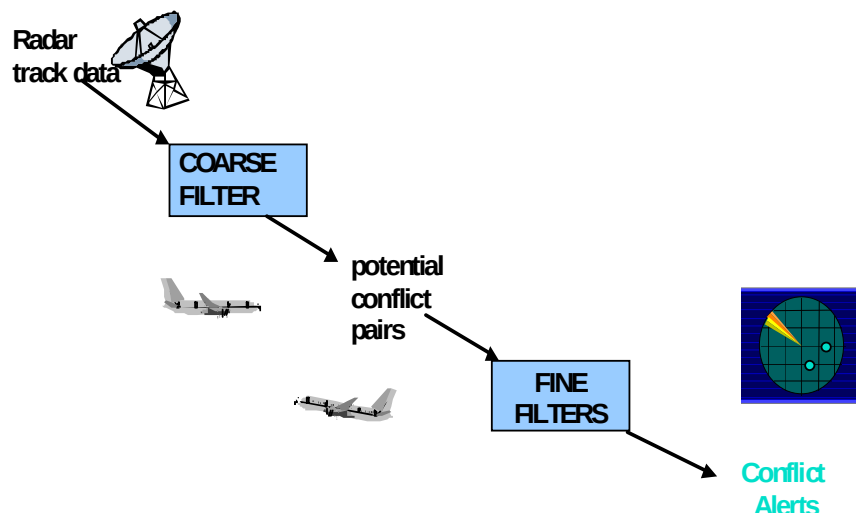


FIGURE 7.1 STCA OVERVIEW

7.4.2 Coarse Filter

The first stage of STCA processing is the coarse filter, which continually scans all radar track data with Mode C present to monitor any pair of aircraft which could potentially come into conflict. The coarse filter has a 'wide' parameter set, meaning it picks up a large number of aircraft pairs, the majority of which will never come into conflict. Once an encounter pair passes certain criteria tests (eg. lateral separation less than 25nm), it is then passed onto the fine filter stage.

7.4.3 Fine Filters

There are three separate fine filters in the STCA system. Each assesses the risk of a separation loss in a different way, and any one filter can trigger an alert depending on the particular circumstances.

STCA runs an encounter pair through the fine filters once every radar cycle. If a pair 'passes' a filter (ie. meets the criteria at which the filter predicts a separation loss may occur) it generates a 'hit' for that cycle. Generally, each filter requires a given number of hits over a set number of cycles before the filter is 'confirmed'. Only once a filter is confirmed does the encounter move onto the final stage of processing which is the alert confirmation stage.

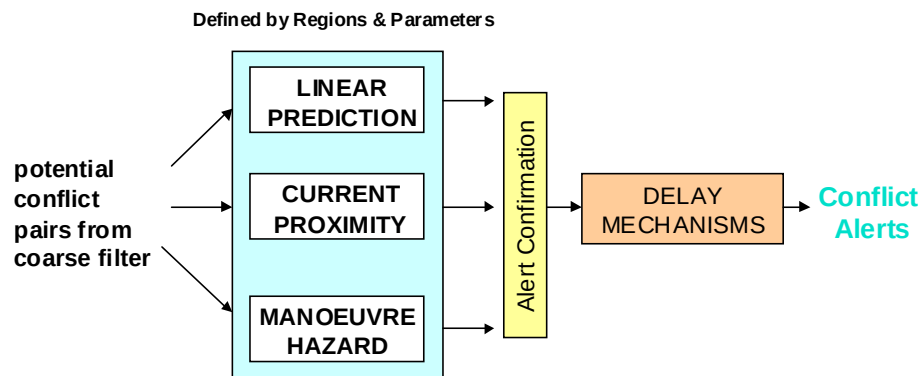


FIGURE 7.2 THE STCA FINE FILTERING STAGE

7.4.4 Linear Prediction (LP) filter

This filter looks at the previous track of the aircraft and extrapolates forward in time to predict where the aircraft will be in the future. If the linear prediction filter estimates that two aircraft will come into conflict within a timeframe, a hit on the linear prediction filter is registered.

7.4.5 Current Proximity (CP) filter

This filter uses the current positions of each aircraft and calculates the lateral and vertical separation at that moment. If these separations fall below a given value, a hit on the current proximity sliding window is generated.

7.4.6 Alert Confirmation

The third and final stage of STCA processing is alert confirmation. This consists of a number of tests which can either cause an alert to be generated earlier than normal, or to delay the alert.

GUIDANCE: Up to this point, this section contains an overview of STCA and how it works. It is likely that most ANSPs will have a similar system at this level, and it may be possible for them to base their description on this text with appropriate modifications.

ANSPs will need to augment this section with a reference to the design description of the actual STCA system, and show how that design implements all the requirements. This might be achieved by a traceability matrix, for example.

7.5 The Technical System is implemented and integrated as Designed [Arg 3.2]

ILLUSTRATIVE EXAMPLE:

The technical system is implemented in hardware and software and integrated into the host surveillance system as designed. The evidence for this comes from reviews, testing, analysis etc.

7.5.1 Assurance for the implementation and integration

GUIDANCE: Assurance that the technical system has been implemented in accordance with the design will be intimately dependent on the actual design, the implementation and the processes. Assurance is likely to be made up of evidence from the engineering processes followed, the results of testing, and controller-in-the-loop simulations. [Safety Plan Ref: 7.3.1]

The STCA algorithms are complex and are likely to be difficult to verify completely using simple functional tests. Test scenarios based upon extracts from recordings of real radar data might be used and the resulting data compared an off-line model. Evidence may be available from a corrective action system based on reported defects.

The operational performance of STCA is likely to be highly dependent upon the correct choice of adaptation (i.e. adapted for the procedures in use in the relevant volumes of airspace). This is likely to iterate during development and testing, and may again provide evidence of evolutionary correctness.

The achievement of more subjective requirements such as controller acceptability and usability is likely to be obtained in controller-in-the-loop simulations and trials.

Ultimately, it is unlikely that overwhelmingly compelling evidence is available without the collection of in-service data – where STCA will be operating in the real operational environment. In service monitoring and adaptation will probably need to be carried out. This may affect the initial operational use of the STCA system (see Section 9 – Conclusions)

7.5.2 Summary of Assurance in the Design

GUIDANCE: Summarise the evidence in each category, and the assurance that they provide that the design has been correctly implemented.

7.6 STCA Procedures Designed and implemented to meet the requirements [Arg 3.3]

ILLUSTRATIVE EXAMPLE:

The procedures have been designed taking full cognisance of the controllers and engineers point of view and related human factor issues. A Human factors expert has been consulted in the process to ensure that there is limited scope for ambiguity in understanding in the procedures.

The procedures have been implemented and integrated into the ANSP documentation set as designed.

GUIDANCE: Procedures for the operation of STCA will need to be defined to ensure that operational requirements are met. Evidence will need to be presented that the combination of environment, the procedures and the design of the equipment together ensure that the requirements are met. [Safety Plan 7.2.4, 7.2.5 & 7.2.6].

Reversionary procedures will also need to be defined for those circumstances where STCA is not performing correctly.

Evidence will need to be presented to show that those procedures have been implemented. [Safety Plan 7.3.3].

7.7 Training Courses for Controllers and Engineers designed and implemented to meet the requirements [Arg 3.4]

ILLUSTRATIVE EXAMPLE:

Training courses for operation and maintenance of STCA have been designed and documented (include document references). Controllers and Engineers have been trained and are deemed to be competent to operate the system and procedures.

Training courses for controllers and engineers have been implemented as designed.

GUIDANCE: Evidence will need to be presented to show that any training necessary for controllers or engineers to be able to operate and maintain the equipment has been identified, appropriate training courses developed, [Safety Plan 7.2.3 & 7.4.4] and that staff have successfully completed those courses. [Safety Plan 7.3.2]

7.8 Safety Requirements for the Transfer to operations specified [Arg 3.5]

ILLUSTRATIVE EXAMPLE:

A safety assessment has been carried out to ensure that the existing ATM system will not be put at risk during the integration and transfer to operations of a new system - people, procedures and equipment included. The assessment was made to identify any potential hazards that might need to be mitigated during that phase of activity.

The assessment involved relevant ATC and engineering staff. The main hazard highlighted was that the new software might be run inadvertently in the operational radar system causing to fail. The resulting safety requirement relates to ensuring that the part of the system being worked on is completely isolated from the operational system during this phase. This activity must be reinforced by management supervision and control.

GUIDANCE: Safety requirements must be defined associated with managing the risks to the ongoing ATC operations resulting from putting the STCA system into operation. These safety requirements will result from a hazard analysis of the technical and operational impacts of the transfer to operations.

This section is likely to comprise a list of the hazards (and a rationale that they indeed are the hazards), an analysis of the hazards for their impact on the operation, and a series of transition requirements developed to manage the risk down to a tolerable level. [Safety Plan 7.3.4].

8. SYSTEM TRANSITION, OPERATION & MAINTENANCE

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

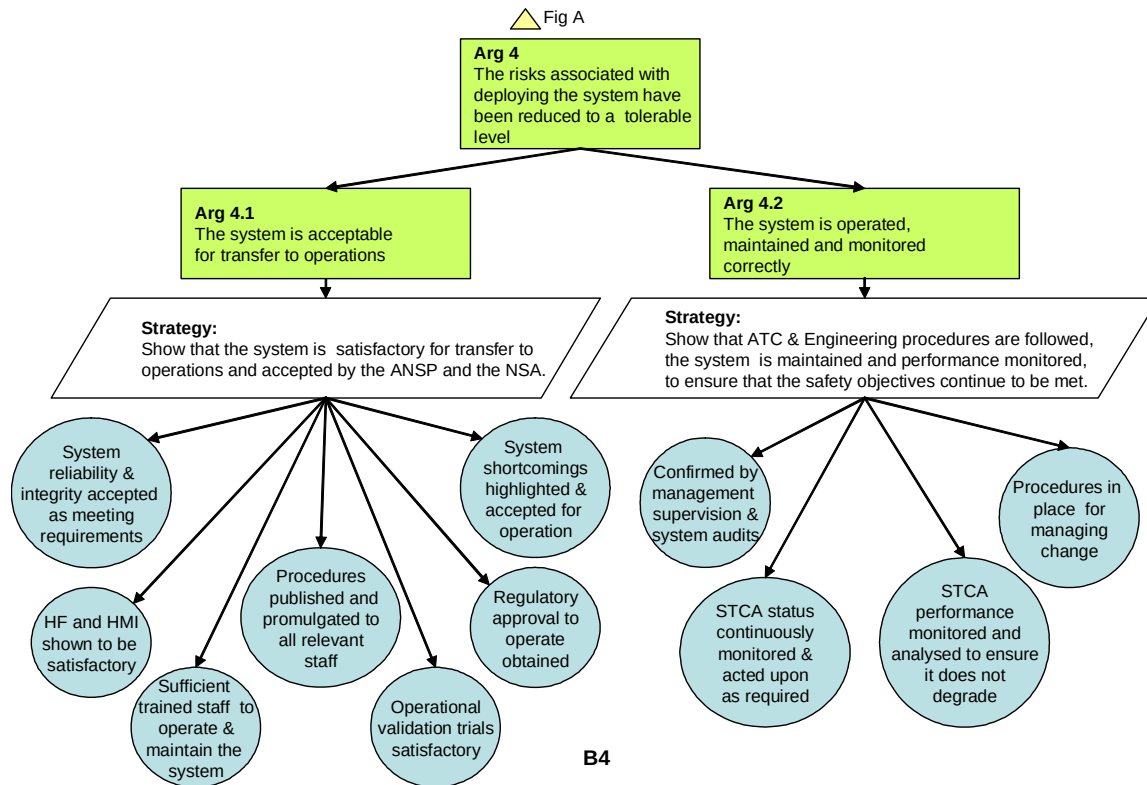


FIGURE B4 SYSTEM OPERATION & MAINTENANCE ASSURANCE

8.2 Transfer to Operations

GUIDANCE: The assurance activities are listed in Table 7.4 of the Safety Plan.

8.3 Operation and Maintenance

GUIDANCE: STCA status information is continuously monitored and Controllers are advised of any changes that might affect the system performance.

STCA performance is monitored and analysed to ensure that it does not degrade and that it continues to satisfy ANSP safety objectives.

The assurance activities are listed in Table 7.5 of the Safety Plan.

9. CONCLUSIONS

GUIDANCE: Conclude with a statement that the top-level Claim has been satisfied, subject to the caveats below – assumptions, shortcomings, limitations and outstanding safety issues. Provide a quantified level of the degree of the net safety benefit provided, if possible.

Further guidance on safety case Conclusions can be found in the EUROCONTROL SCDM.

9.1 Assumptions

GUIDANCE: List any key assumptions that have had to be made in the safety case, or underlying safety assessment. Explain why these assumptions have had to be made and why it is believed that the assumptions are valid (or at least reasonable).

9.2 Shortcomings

GUIDANCE: List as shortcomings any cases where the safety requirements have not been met, or where there is limited confidence that they have been met. For each case, determine and justify whether the overall safety objectives are compromised by the failure to meet the requirement.

For example, if there were circumstances under which a large number of erroneous STCAs being displayed that would represent a shortcoming against the requirements.

9.3 Limitations

GUIDANCE: For each shortcoming that has an operational impact, identify the nature of that impact, the residual risk it represents, and any agreed operational mitigations that could be put in place to reduce that risk. Confirm that the ANSP has accepted the limitation and the need for the mitigation.

For example, in the case illustrated above, the STCA function could be withdrawn temporarily from service until the problem causing the alerts was resolved - loss of the STCA function being preferable to erroneous performance.

9.4 Outstanding Safety Issues

GUIDANCE: List any outstanding issues that need to be resolved before the safety case can be considered to be completed. Show what actions need to be, preferably have been, put in place to resolve them.

END OF DOCUMENT