EUROCONTROL

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

Edition Number	:	2.0
Edition Date	:	19 May 2009
Status	:	Released Issue
Intended for	:	CND Stakeholders

EUROCONTROL

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidance Material for Short Term Conflict Alert **Appendix B-3 Outline Safety Case for STCA System**		
Document Identifier	**Edition Number:**	2.0
EUROCONTROL-GUID-123	**Edition Date:**	19 May 2009

Abstract

This document is part 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
STCA
Safety Argument
Safety Plan
Safety Case

Contact Person(s)	Tel	Unit
Hans Wagemans	+32 2 72 93334	CND/COE/AT/AO

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

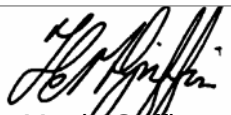
ELECTRONIC SOURCE		
Path:	\\HHBRUNA02\bakkerb$\QC	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	720 Kb

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	 Hans Wagemans	19-5-2009
Head of ATC Operations and Systems Unit	 Martin Griffin	19-5-2009
Deputy Director Network Development	 Alex Hendriks	19-5-2009

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	14-12-2006	First released issue	All
2.0	19-5-2009	Alignment with updated EUROCONTROL Specification for STCA and latest Safety Assessment Methodology	All

CONTENTS

EXECUTIVE SUMMARY

It is Safety Management best practice and an ESARR 4 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 Supervisory Authorities (NSA) 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. Each document represents a snapshot of the safety assurance work already undertaken at different stages of a project. The document set includes:

1. **Initial Safety Argument for Short Term Conflict Alert**: - Ideally, produced during the definition phase of a project to introduce a change to the ATM system e.g. to introduce STCA. The process of developing and acquiring the necessary assurance is considerably enhanced if the safety arguments are set out clearly from the outset.

2. **Generic Safety Plan for the implementation of STCA**: - Initially produced at the outset of a project as part of the project plan, but focused only on those activities necessary to provide assurance information for inclusion in a safety case. The safety plan will be subject to development and change as the project unfolds and more detail becomes available.

3. **Outline Safety Case for STCA** [This document]:- Commenced at the start of a project, structured in line with the safety argument, and documented as the results of the planned safety assurance activates become available.

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. This corresponds to the Functional Hazard Assessment (FHA) and the Preliminary Safety Assessment Process (PSSA) in SAM. 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.

Note: This is guidance material only – It is not intended to demonstrate that STCA is safe. It requires effort from the ANSP to transfer this outline case into a complete safety case.

1. INTRODUCTION

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

The European Convergence and Implementation Plan (ECIP) contain a pan-European Objective (ATC02.2) for ECAC-wide standardisation of STCA in accordance with the EUROCONTROL Specification for Short Term Conflict Alert. The document specifies, in qualitative terms, the common performance characteristics of STCA as well as the prerequisites for achieving these performance characteristics.

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.

A Safety Case is the documented assurance 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,*** and the Regulator, that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety.

2. PURPOSE OF THIS DOCUMENT

The purpose of this document is to illustrate through examples an outline structure for a safety case that can be used by ANSPs in documenting safety assurance for STCA applications. 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) [Ref 7].

The overall approach for developing the safety case is shown in Figure 2-1[1] below. The safety assurance objectives (what has to be done) and activities (how the objectives are achieved) to be accomplished in the subsequent phases of the lifecycle are determined from the safety argument and the safety plan. The evidence that the assurance objectives have been achieved is obtained from the SAM Functional Hazard Assessment (FHA), Preliminary Safety Assessment (PSSA), and the System Safety Assessment (SSA) and presented in the Safety Case.

[1] Figure 2-1 and the associated text is adapted from the document: Safety Assessment Made Easier [Ref 4]

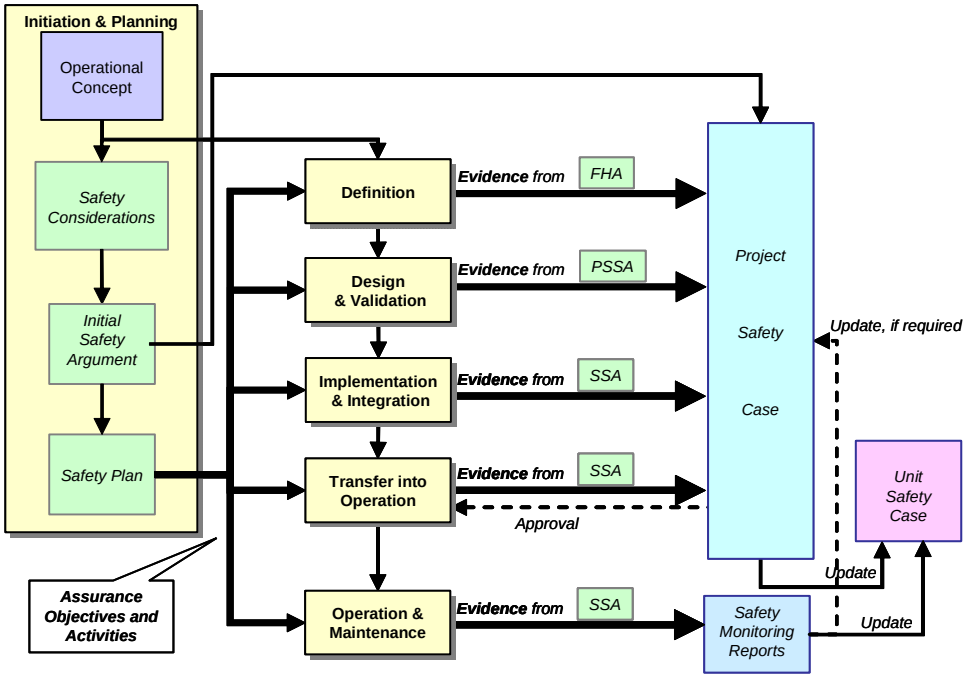


Figure 2-1: Overall Approach

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 show that STCA will be acceptably safe in ATM operations. The arguments and the evidence to give this assurance are presented in document.

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. Throughout this document references to the chapters in the safety plan are indicated as follows [Safety Plan 7.1.1].

The Safety Case is derived from the overall argument structure described in the document, “Initial 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 support it.

GUIDANCE: STCA is a function provided within the surveillance system and is 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 Diagram 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 STCA development and the safety case development. Each of the arguments has to be satisfied in order to make the safety case.

4.2 Safety Argument and Evidence Sections

The following sections present each of the strands of the safety arguments in turn, together with the evidence to show that each of the arguments is met. The assurance objectives (as determined from the Initial Safety Argument and the Safety Plan) are given in a table following each argument, together with a summary of the evidence to be found in the safety case.

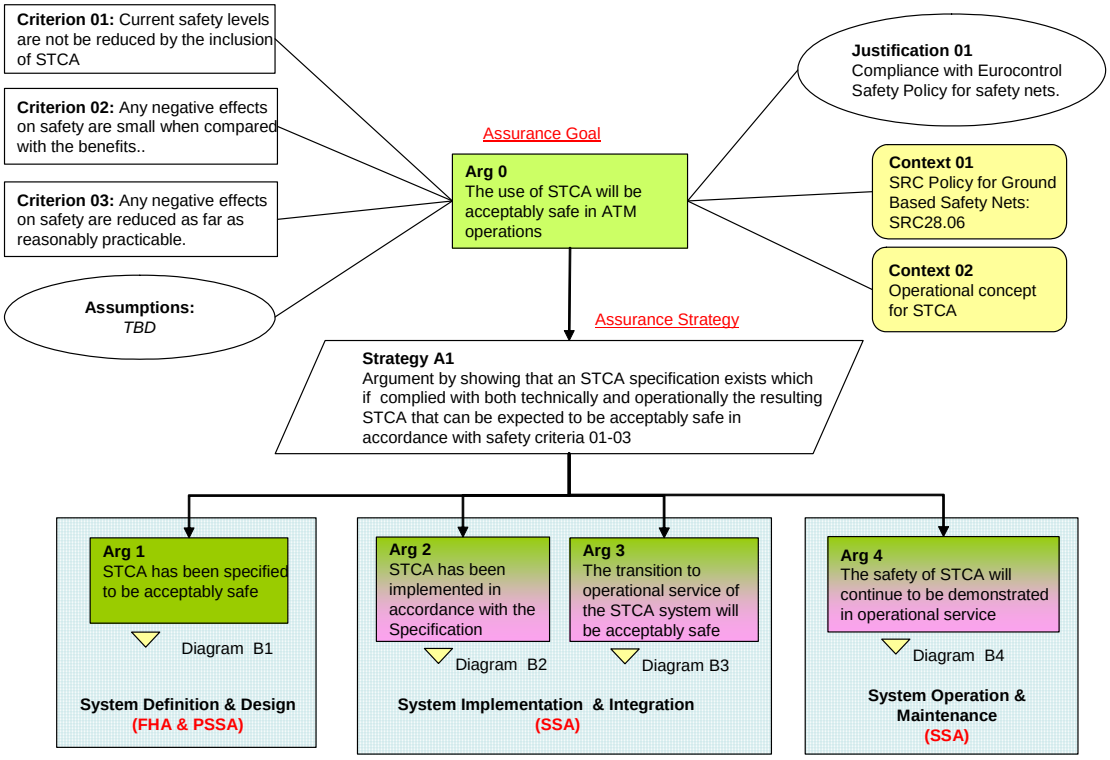


Diagram A: Overall Argument Structure

Note: Where GSN is used in the document the argument symbols have different colours to reflect the degree to which the particular argument has been addressed in this Outline Safety Case. "Green" indicates that the argument and evidence is reasonably well developed. "Green/Pink" indicates that the argument is only partly addressed, or not at all.

4.3 Top Level Argument [Arg. 0]

The top-level argument for which assurance is required is that "STCA will be acceptably safe in ATM operations".

4.4 Criteria

GUIDANCE: The criteria for deciding what will constitute "acceptably safe" have to be established at the outset.

Criteria for judging if STCA is acceptably safe are:

- **CRITERION 01**, current levels of safety are not reduced by the inclusion of STCA *i.e. there is no net increase in the number of incidents above current levels as result of installing and operating STCA.*

Note: Criterion 01 cannot be shown to be met until STCA has been implemented.

- **CRITERION 02,** any negative effects on safety are small compared with the safety benefit *i.e. that the number of incidents contributed to by STCA is small compared to the number resolved by ATC as a result of an STCA Alert.*

- **CRITERION 03,** any negative effects on safety are reduced as far as reasonably practicable *i.e. this criterion points to the need to include mitigation means to ensure that the number of incidents contributed to by STCA is small, and consistent with the requirements of criterion 02.*

GUIDANCE: Depending on ANSPs safety management arrangements and regulatory arrangement, it is possible that some ANSPs will wish to provide quantifications of these criteria [Safety Plan 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 2:

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

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

4.5 Context

In addition to meeting the above criteria, STCA will also need to be deemed acceptably safe in relation to the Safety Regulation Commission (SRC) Policy for Safety Nets [Safety Plan 7.1.2].

4.5.1 Context 01 Safety Policy for STCA

The EUROCONTROL SRC acknowledges that ground based safety nets are part of the ATM system and contribute positively to its safety [Ref 5]. As STCA is classed as a ground based safety net, this policy is relevant to this safety case.

The EUROCONTROL Specification for STCA has provided generic policy statements to which are consistent with the SRC Policy, 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"

GUIDANCE: This Outline Safety Case is based on the EUROCONTROL Specification for STCA, and hence the policy it describes.

4.5.2 Context 02 Concept of Operation for STCA

The Concept of Operations (Conops) upon which this Outline Safety Case is based was developed by the SPIN Task Force. The Conops is included in the EUROCONTROL Specification for Short Term Conflict Alert [Ref 1]. For STCA to be acceptably safe, the Conops itself needs to be safe. An argument to that effect is included in this document.

4.6 Assumptions

GUIDANCE: ANSPs should include here any assumptions on which the top level argument is dependent e.g. the host surveillance system is acceptably safe [Safety Plan 7.1.3].

4.7 Strategy A1

The main strategy adopted to meet Arg 0 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 and 03. 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.

4.8 Justification 01

Compliance with EUROCONTROL Safety Policy as expressed in the EUROCONTROL Specification for STCA is necessary to justify the argument that STCA will be acceptably safe. This policy is reflected in the Criteria 01, 02 and 03.

5. STCA SPECIFICATION AND SAFETY REQUIREMENTS

5.1 Assurance Evidence

Evidence is required from the System Definition and Design phase to demonstrate that **Arg 1** can be considered to be true i.e. that STCA has been specified to be acceptably safe. The strategy followed to show that **Arg 1** can be considered to be true is shown in Diagram B1, together with sub-arguments (Arg 1.1 to Arg 1.7) and pointers to the Tables listing the safety assurance objectives to be addressed.

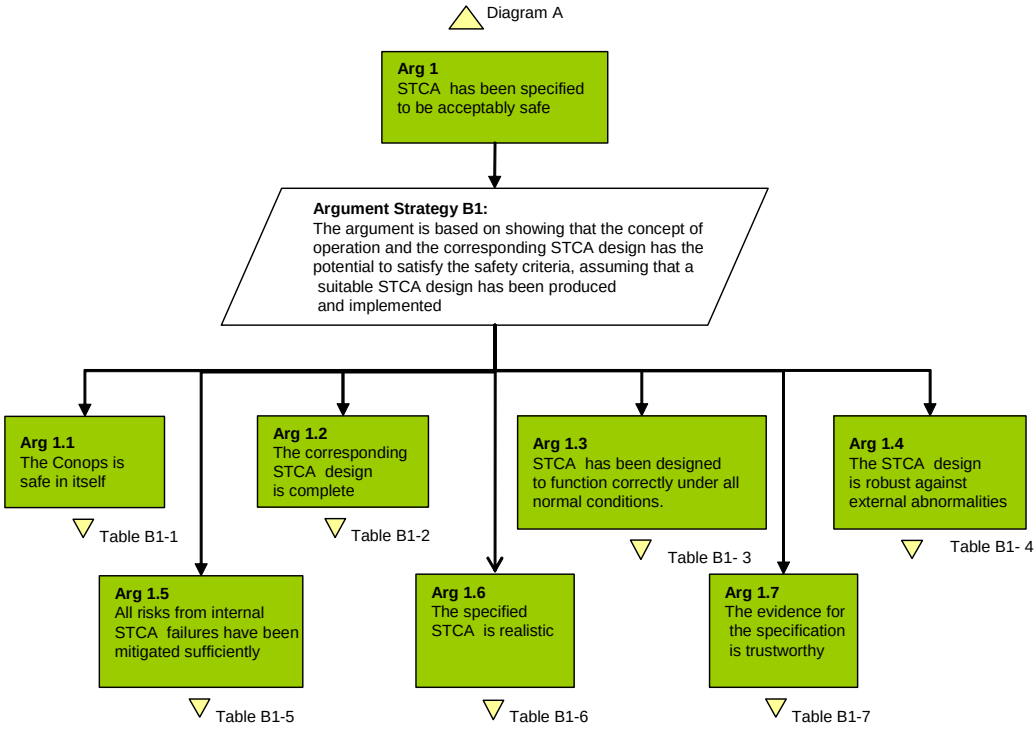
[2] This is the adapted form recommended by the EUROCONTROL SCDM.

The safety assurance objectives to be addressed, and for which evidence is required, are shown in a Table under each argument heading, together with summary of the evidence offered in this safety case.

The safety assurance objectives are based on the assurance objectives in Safety Assessment Made Easier [Ref 4].

GUIDANCE: Arguments 1.1 to 1.4 are concerned with the success of STCA in contributing to ATM safety i.e. in addressing pre-existing hazards. The specified functional and non-functional requirements for STCA determine how safe it needs to be in the absence of failure and are therefore regarded as STCA safety requirements. Note: As stated previously, these safety requirements are distinct from, and in addition to, those derived under argument 1.5 below.

Argument 1.5 is concerned only with the consequences of failure of STCA (i.e. new hazards) and leads mainly to a specification of Safety Objectives[3] and Safety Requirements[4] for the integrity of the system.



B1

Diagram B1: STCA Specification Argument

5.2 The Conops is safe in itself [Arg 1.1].

The Concept of Operation (Conops) describes what STCA is intended to achieve operationally, and defines the key functionality and performance parameters and how it is to be used. The assurance issue is whether the

[3] Safety Objectives is a term used in ESARR 4 and in Eurocontrol Safety Assessment Methodology to describe the maximum tolerable occurrence rate of hazards.
[4] Safety Requirements refer to the mitigation means for hazards

underlying concept is capable of satisfying criteria 01, 02 and 03, assuming that a suitable design could be produced and implemented [Safety Plan 7.1.4]. The assurance objectives to be addressed to satisfy Arg 1.1 are shown in Table B1-1, together with summary of the evidence offered in this safety case.

Arg 1.1 – Assurance Objectives	Evidence Summary
(1) Show that the initial safety issues have been identified and addressed.	The draft Conops has been subject to formal review and modified to mitigate any hazards identified. See paragraph 5.3.
(2) Show that the minimum functionality has been defined and shown to be compatible with Safety Criterion 02 and 03.	The argument and evidence is described in paragraph 5.3
(3) Show that the differences from existing Conops have been described, in terms of what STCA will do when introduced into the ATM system.	The “existing system” referred to here is the non-STCA ATM system. The Conops describes what STCA will do when introduced into the system.
(4) Show that the impact of the Conops on the operational environment (including interfaces with adjacent systems / airspace) has been assessed and shown to be compatible with safety criteria 02 and 03.	The areas to be considered are identified in the Conops and the EUROCONTROL Specification. However, it is a matter for the ANSP to assess the actual impact on their system.

Table B1-1: Assurance Objectives to satisfy Arg 1.1

5.3 The minimum functionality has been defined and shown to be compatible with Safety Criterion 02 and 03.

STCA is not a new concept; it has been used operationally for many years. However, a survey of carried out by EUROCONTROL in 2004 by the European Safety Programme (ESP) Activity Field 4[5] revealed that most existing STCA implementations are inherently capable of functioning as efficient safety nets but that the existing capabilities are not always used effectively. The survey identified 14 areas of concern affecting all aspects of STCA operation. This led to the establishment of the Safety nets: Planning Implementation and eNhancements (SPIN) Task Force in 2005 to develop standards and supporting guidance material for safety nets, including STCA. The work involved 11 ATS providers, 5 industrial suppliers and the EUROCONTROL Agency in the development of the material.

The Task Force produced a draft specification for STCA and this was subject to formal consultation by EUROCONTROL Member States using the EUROCONTROL Notice of Proposed Rule-Making (ENPRM) process[6]. 12 Stakeholders contributed to the process. The document was finalised in November 2007 and Edition 1 was approved by EUROCONTROL DG.

[5] SPIN: Survey of Practises in Safety Nets; Summary report Edition 1.01 [Ref 6]
[6] Summary of Responses (SOR): Report on Formal Consultation on STCA 6 June – 5 September 2007.

The STCA Specification developed by the SPIN Task Force includes the Concept of Operation and the key (minimum) functionality and performance parameters for STCA.

The key factors necessary for safe and effective use of the Concept are addressed and include:

- STCA policy
- Human Factors
- Design
- Technical aspects
- Interactions with other Safety Nets
- Provision for future directions

Significant amongst these from a safety point of view are:

- STCA policy, whereby the *sole purpose (of STCA) is to enhance safety and its presence is ignored when calculating sector capacity"*. This means that the Controller is not to rely on it for maintaining safe separation, and so it is safe by definition in that regard.
- The Conops is designed to ensure that urgent alerts are notified immediately, with a warning time of up to 2 minutes, and that nuisance alerts are minimised.
- The requirements for training and awareness of controllers in the operation of STCA
- The importance of monitoring the performance of the system and optimising it to maintain effectiveness

5.3.1 Conclusions

Based on the documented and thorough process followed by the SPIN task force in developing the STCA Specification and Conops, and the expert judgement and operational experience of STCA of those involved, it is concluded that the Conops and the Specification has the potential to meet the safety criteria.

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 the top level argument 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.

5.4 The corresponding STCA design is complete [Arg 1.2]

5.4.1 Assurance Evidence

The assurance issue here is whether everything necessary to achieve a safe implementation of the Concept has been specified in the EUROCONTROL Specification [Safety Plan 7.1.5].

GUIDANCE: ANSPs will need to have functional and non-functional requirements for STCA appropriate to their concept of operation and operational environment. This will inevitably be more detailed than the EUROCONTROL Specification. The Guidance Material for STCA, appendix A: Reference STCA System [Ref 3] provides detailed guidance in this regard.

The Assurance objectives to be addressed to satisfy Arg 1.2 are shown in Table B1-2, together with summary of the evidence offered in this safety case.

Arg 1.2 – Assurance Objectives	Evidence Summary
(1) Show that everything necessary to achieve a safe implementation of the Conops – related to human, procedure, equipment and airspace design - has been specified.	The function and non-functional requirements from the EUROCONTROL Specification are mapped on to the Conops. These are shown to be consistent with the Conops by reference to the tables B1-2a to B1-2g
(2) Show that all the safety requirements on and assumptions about, external elements of the STCA have been captured.	The STCA specification has been formally reviewed to ensure that it covers external elements of STCA. *The ANSP will have to provide this assurance in relation to their STCA system.*

Table B1-2: Assurance Objectives to Satisfy Arg 1.2

5.4.2 Functional and non-functional safety requirements

As the whole objective for STCA is to reduce risk in ATM, the functional and non-functional requirements[7] specified in the EUROCONTROL Specification for Short Term Conflict Alert [Ref 1] are, by inference, safety requirements. These relate to the "success case" – i.e. that STCA will be acceptably safe in the absence of failure[8]. Note: These safety requirements are distinct from and in addition to those derived under Arg 1.5.

[7] **Functional requirement**s specify what the system should do. **Non-functional requirements** specify how a system must behave; they are a constraint upon the systems behaviour. Typical non-functional requirements are performance, throughput, utilisation etc.

[8] Refer to EUROCONTROL SAM Part 1

(1) FUNCTIONAL SAFETY REQUIREMENTS:

Concept of Operation – Functional Safety Requirements: **Conops 3.1:** STCA adds independent alerting logic to the (ATM) 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	Safety Requirement
STCA-07	STCA ***shall*** detect and alert operationally relevant conflicts involving at least one eligible aircraft.
STCA-08	STCA ***shall*** provide alerts for operationally relevant conflicts. (Refer to note in the STCA specification Ch. 4.3.1 for meaning of relevant.)
STCA-09	STCA alerts ***shall*** attract the controller's attention and identify the aircraft involved in the conflict; STCA alerts ***shall*** be at least visual.
STCA-13	STCA ***shall*** continue to provide alert(s) as long as the alert conditions exist.
STCA-14	STCA ***shall*** provide the possibility to inhibit alerts for predefined volumes of airspace and for individual flights. (Refer to the STCA specification and the guidance material for more details on this function).
STCA-15	Alert inhibitions ***shall*** be made known to all controllers concerned.
STCA-16 SRC Policy Ch. 5.3.(8)	Status information ***shall*** be presented to supervisor and controller working positions in case STCA is not available. Users ***should*** be aware of the availability and operational status of ground based safety nets in real time
STCA-18	All pertinent STCA data ***shall*** be made available for off-line analysis. (Refer to STCA guidance material appendix A for guidance on pertinent data)

Table B1-2a: Mapping functional safety requirements

(2) NON-FUNCTIONAL SAFETY REQUIREMENTS:

Concept of Operation - Procedures Safety Requirements: Not addressed explicitly in the Conops, but the following safety requirements are relevant here. [Safety Plan 7.1.8 and 7.1.11]	
Req No	Safety Requirement
STCA-04 (paraphrased)	Local instructions concerning the use of STCA ***shall*** be specified. See STCA specification for further details of the requirement.
STCA-05	In the event an alert is generated in respect of controlled flights, 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.

Table B1-2b: Mapping safety requirements

Concept of Operation - System Boundaries and Environment Functions:	
STCA may need to take into account the specific volume of airspace in which each aircraft is flying, in order to apply appropriate parameters or trajectory predictions. Different parameters may be applied in the case of system degradation (e.g. unavailability of one or more radar stations) [Ref 1 Chap 4.3.5]. In RVSM airspace, STCA should be able to selectively assess the applicable vertical separation minimum of either 300 m (1000 ft) or 600 m (2000 ft), as determined by the current RVSM approved or non-approved (incl. unknown and exempt) status of the flight concerned. [Ref 1 Chap 4.3.5] and [Safety Plan 7.1.4]	
Req No	Safety Requirement
STCA–A1	STCA ***should*** be adaptable for the procedures in use in all distinct volumes of airspace at any moment in time.
STCA–A2	STCA ***may*** need to take into account the specific volume of airspace in which each aircraft is flying, in order to apply appropriate parameters or trajectory estimation. Different parameters ***may*** be applied in the case of system degradation (e.g. unavailability of one or more radar stations).
STCA–A3	In RVSM airspace, STCA ***should*** be able to selectively assess the applicable vertical separation minimum of either 300 m (1 000 ft) or 600 m (2 000 ft), as determined by the current RVSM approved or non-approved (incl. unknown and exempt) status of the flight concerned.

Table B1-2c: Mapping safety requirements

Concept of Operation - Performance Safety Requirements:	
Conops 3.1: STCA is intended to function in the short term, if applicable providing warning times up to 2 minutes. **Conops 3.2:** 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 hazardous situations, governed by the inherent characteristics of the human centred system.	
Req No	Safety Requirement
STCA-10	The number of nuisance alerts produced by STCA ***shall*** be kept to an effective minimum. Note: what constitutes an effect minimum will be decided on factors such as the impact on controller workload, and whether resolution and/or recovery functions are impaired in any way. See also Appendix A for additional guidance in this regard.
STCA-11	The number of false[9] alerts produced by STCA ***shall*** be kept to an effective minimum. See Note above.
STCA-12	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.

Table B1-2d: Mapping performance safety requirements

[9] 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).

Concept of Operation – Monitoring Performance Safety Requirements:	
STCA Specification 4.2.4: The appropriate ATS authority should retain electronic records of all alerts generated. The data and circumstances pertaining to each alert should be analysed to determine whether an alert was justified or not. Non-justified alerts, e.g. when visual separation was applied, should be ignored. A statistical analysis should be made of justified alerts in order to identify possible shortcomings in airspace design and ATC procedures as well as to monitor overall safety levels.	
Req No	Safety Requirement
STCA-06	STCA performance ***shall*** be analysed regularly to identify possible shortcomings related to STCA.

Table B1-2e: Mapping performance safety requirements

Concept of Operation – Policy	
Conops 3.2: 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. The following Functional and Performance Safety requirements should be reflected in the policy. See EUROCONTROL Guidance Material for STCA [Ref 2] for further guidance on policy and also [Safety Plan 7.1.2].	
Req No	Safety Requirement
SRC Policy 5.1 (bullet points 2 and 3).	STCA is a Safety Net, and ***should*** not to be designed or relied upon as a sole means of means of potential mitigation for identified hazards.
SRC Policy 5.3 (bullet point 9)	STCA users ***should*** be aware that the safety of the service is predicated on their continuing to ensure separation without relying it.
STCA - 01	The ANSP ***shall*** have a formal policy on the use of STCA consistent with the operational concept and safety management system applied to avoid ambiguity about the role and use of STCA.
STCA - 02	The ANSP ***shall*** assign to one or more staff, as appropriate, the responsibility for overall management of STCA.

Table B1-2f: Mapping safety requirements

Concept of Operation – Training and Awareness safety requirements:	
SRC Policy (Recommendations 6.4 and 6.5): In order to ensure correct and effective use of STCA, users should understand the purpose and functioning of STCA, and be aware of its technical availability and operational status. [Ref 5 Chap 5.3] **STCA Specification**: The primary goal of the training is to develop and maintain an appropriate level of trust in STCA, i.e. to make controllers aware of the likely situations where STCA will be effective and, more importantly, situations in which STCA will not be so effective (e.g. sudden, unexpected manoeuvres). [Ref 1 Chap 4.1.3] and [Safety Plan 7.2.3]	
Req No:	Safety Requirement
STCA-03	The ANSP ***shall*** ensure that all controllers concerned are given specific STCA training and are assessed as competent for the use of the relevant to the STCA system.

Table B1-2g: mapping training safety requirements

5.4.3 Conclusions

Based on the above mapping it is concluded that all the necessary functional and non-functional safety requirements relating to equipment, people, procedures and airspace design has been specified to meet the basic Conops. The justification for this conclusion is that the specification was developed by the same expert group who developed the Conops, and the functional and non-functional requirements are complete and consistent with respect to the Conops.

GUIDANCE: Note that the EUROCONTROL Specification sets minimum requirements only, and ANSP specifications are likely to be more specific, especially in relation to non-functional requirements. However, comparison of ANSP specifications with EUROCONTROL Specification can help to determine completeness of the former. Guidance on these issues can be obtained from Guidance Material for STCA Appendix A: reference system [Ref 3].

5.5 STCA has been designed to function correctly under all normal conditions [Arg 1.3]

GUIDANCE: What is required is an outline description of the STCA design showing the relationship between the STCA functions, its boundaries, and the way it will be integrated into the existing ATM system. The level of detail should be sufficient to support the FHA process [Safety Plan 7.1.6].

5.5.1 Assurance Evidence

The assurance issue here is whether the system design can reasonably be expected to achieve the functional and non-functional safety requirements. The Assurance objectives to be addressed to satisfy Arg 1.3 are shown in Table B1-3, together with summary of the evidence offered in this safety case.

Arg 1.3 – Assurance Objectives	Evidence Summary
(1) Show that the STCA design has been clearly described, and has the potential to show that STCA functions correctly under all normal environmental conditions.	The STCA design is described in the following paragraphs, supported by diagrams. *ANSPs may need to include a more detailed description for their system*.
(2) Show that the level of detail is sufficient to support the FHA process and the derivation of safety objectives for the overall design. .	The EUROCONTROL SAM provides guidance on what to include.

Table B1-3: Assurance Objectives to Satisfy Arg 1.3

5.5.2 Outline System Description

A Block Diagram of the STCA system is shown in Figure 5-1. This was derived by reference to the EUROCONTROL Specification for STCA, and in particular to the Conops contained therein. As illustrated in the diagram, STCA obtains information from Surveillance Data Processing and Environment Data Processing. As an option, STCA can additionally make use of data from Flight Data Processing.

- Surveillance data is used to predict conflicts. Tracked mode C data is used to make a prediction in the vertical dimension.
- Environment Data Processing supplies STCA with the necessary parameters for a number of user-defined volumes of airspace.
- Flight data may be used to provide additional information, such as:
  - Type/category of flight: to determine the eligibility for alert generation
  - RVSM status: to apply appropriate parameters in RVSM airspace
  - Sector(s) of concern: to address alerts
  - Cleared/Block Flight Levels: to increase the relevance of conflict prediction

The diagram also illustrates the functions of people, procedures and equipment in the STCA system, and the interfaces between the system elements.

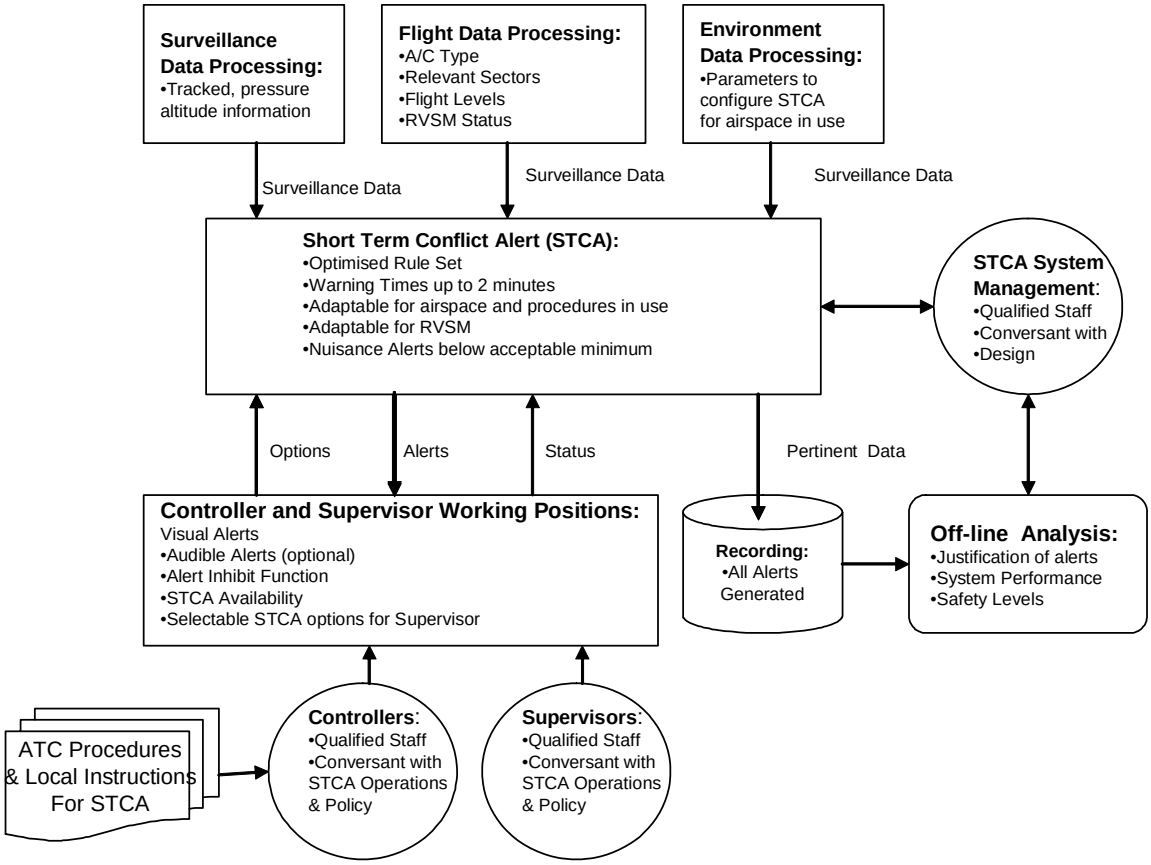


Figure 5-1: STCA System block diagram

5.5.3 STCA System Architecture

GUIDANCE: Include a summary of the system description and how it will operate, in the safety case. This is to aid understanding of the design, and to determine how best to verify and validate it. See below as a sketchy example of what is required.

An outline the STCA system architecture is shown below in Figure 5-2.

The STCA 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 containing flight data and environmental data. 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.

The 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.

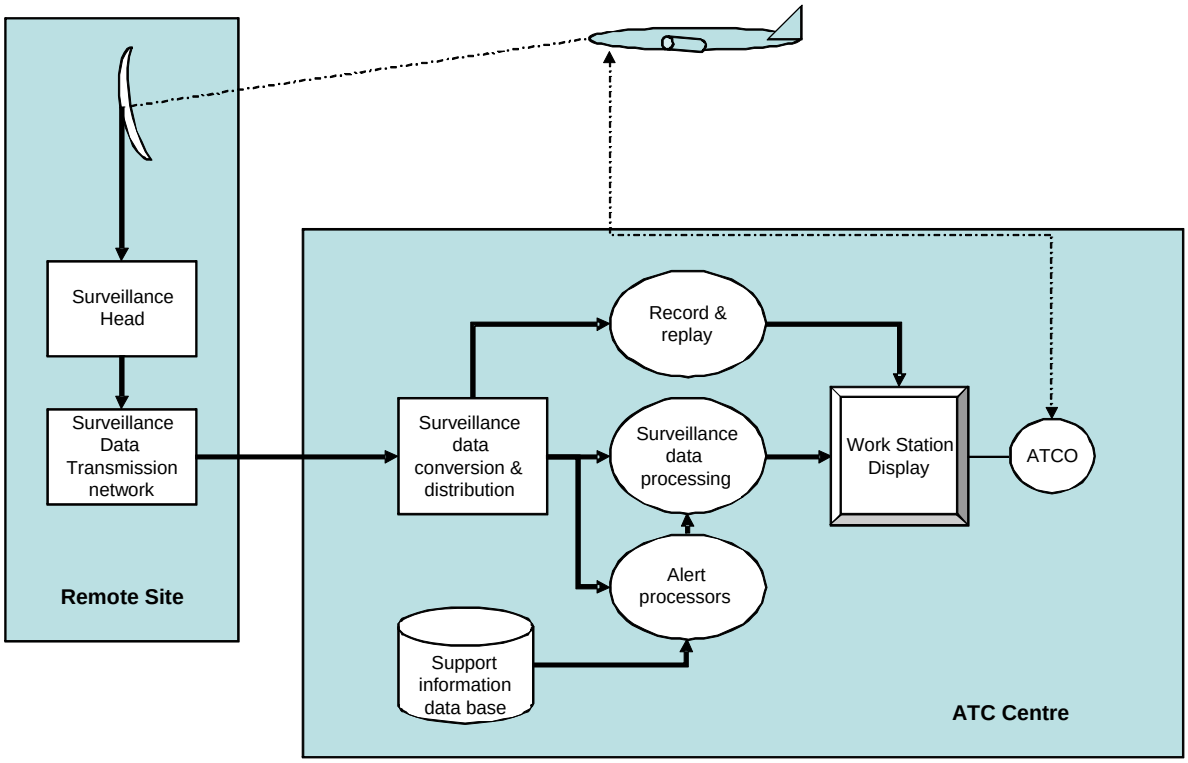


Figure 5-2: STCA System Architecture

5.5.4 STCA Process Model

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.

This following is a high level overview the main features of the design and some of the key parameters used.

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 (e.g. lateral separation less than 25nm), it is then passed onto the fine filter stage.

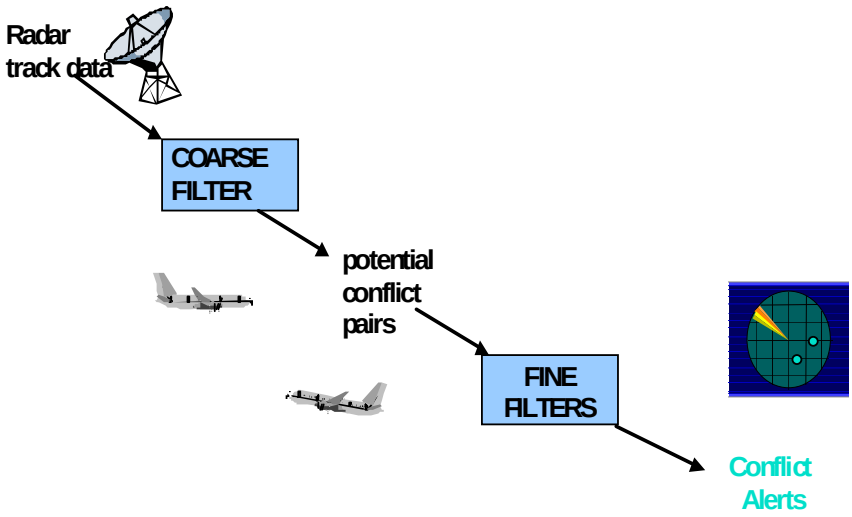


Figure 5-3: STCA Design outline

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 (i.e. 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.

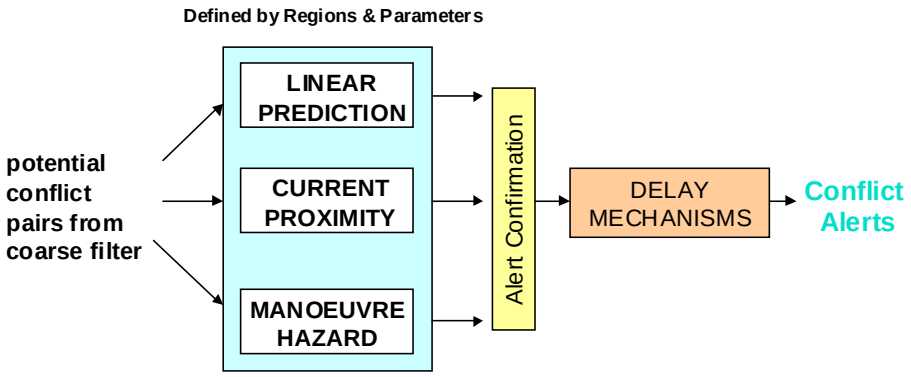


Figure 5-4: The STCA fine filtering stage

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.

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.

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.

5.5.5 Conclusions

Review of the STCA system description and associated diagrams shows that all the elements can be clearly traced to the specified functional and non-functional requirements and that it is complete and correct in this regard. It is therefore concluded that the STCA system as described has the potential to meet the requirements and is sufficient to support the FHA process.

GUIDANCE: This is a summary of the design description, and the complete set of assurance evidence is contained in the design documentation.

5.6 The system design is robust against external abnormalities [Arg 1.4]

The assurance issue here whether the STCA can continue to operate effectively under abnormal conditions in the operational environment or can such conditions cause STCA to behave in a way that could actually induce a risk that would otherwise not have arisen [Safety Plan 7.1.7]. The assurance objectives to satisfy Arg 1.4 are shown in Table B1-4, together with summary of the evidence offered in this safety case.

Arg 1.4- Assurance Objectives	Evidence Summary
(1) Show that the STCA design can react safely to all reasonably foreseeable external failures – i.e. any failures in its environment / adjacent systems that are not covered under Arg1.5.	This is under the scope of the FHA activities carried out under Arg 1.5 and may extend to the ATM boundary. This is for the ANSP to address. *For example, how will STCA react to failure of a navigation aid supporting a holding pattern operated in the STCA environment, making it unusable?*
(2) Show that the STCA design can react safely to all other reasonably foreseeable abnormal conditions in its environment / adjacent systems that are not covered under Arg1.3.	This is for the ANSP to address. *For example, how will STCA react to radar ghosting whereby a multipath signal return incorrectly appears to the radar receiver as a valid target?*

Table B1-4: Assurance Objectives to Satisfy Arg 1.4

5.7 All risks from internal STCA failures have been mitigated sufficiently [Arg 1.5]

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 is to apply the FHA/PSSA processes 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 7.1.8].

This process leads to the specification of Safety Objectives and Safety Requirements for the integrity of the system that can be expected to satisfy Criterion 02.

5.7.1 Assurance Evidence

In compliance with ESARR 4 [Ref 9] it is necessary to ensure that the risks associated with hazards stemming from implementing STCA are systematically and formally identified, assessed and managed, within acceptable levels, prior to its introduction into operational service. [Ref 5 SRC Policy]

The concern here is with the internal behaviour of STCA, from two perspectives: how loss of functionality could reduce the effectiveness of STCA as a safety net; and how anomalous behaviour of STCA could induce a risk that might otherwise not have arisen pre STCA.

The Assurance Objectives to satisfy Arg 1.5 are shown in table B1-5, together with summary of the evidence offered in this safety case.

Arg 1.5- Assurance Objectives	Evidence Summary
(1) Show that the all reasonably foreseeable hazards, at the boundary of the system, have been identified	Addressed in paragraphs: 5.7.2 (hazard identification); 5.7.3 (scope of FHA); 5.7.4 (process), FHA Results (Table B1-5a).
(2) Show that the severity of the effects from each hazard has been correctly assessed, taking account of any mitigations that may be available / could be provided external to the system	Addressed in FHA Results (Table B1-5a)
(3) Show that the Safety Objectives have been set for each hazard such that the corresponding aggregate risk is within the specified Safety Criteria	Paragraph 5.7.6 and FHA Results (Table B1-5b) *ANSP to assign probabilities*
(4) Show that the all reasonably foreseeable causes of each hazard have been identified	See paragraph 5.7.7 (hazard causes) and the Fault Tree (Figure 5-6)
(5) Show that the Safety Requirements have been specified (or Assumptions stated) for the causes of each hazard, taking account of any mitigations that are / could be available internal to the system, such that the Safety Objectives (and/or Safety Criteria) are satisfied	See paragraph 5.7.9 and tables B1-5c, B1-5d and B1-5e. *ANSP to assign probabilities*
(6) Show that the Safety Requirements have been verified and validated.	See assurance evidence in table B1-6
(7) Show that the all external and internal mitigations have been captured as either Safety Requirements or Assumptions as appropriate	See for example Safety Objective 08 relating to loss of STCA
(8) Show that the STCA can actually operate safely under all degraded modes of operation identified under this Argument	Not fully addressed in the PSSA but would include issues such as e.g. • degraded algorithms and system parameters, • Loss of Mode C or Mode S where used) • Loss of radar resulting in loss of multi-track capability

Table B1-5: Assurance Objectives to Satisfy Arg 1.5

5.7.2 Hazard Identification

GUIDANCE: To assess the risk arising from internal failures of the system 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 and Preliminary System Safety Assessment. The FHA and PSSA processes followed were those defined in the EUROCONTROL SAM.

It is essential that those involved in the hazard identification process are properly qualified for the purpose. Guidance in this regard is given in SAM FHA Guidance Material B1 and B2.

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

The functions specified in the EUROCONTROL Specification for STCA were subjected to Functional Hazard Assessment 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 assessment was conducted as a desktop exercise by suitably qualified safety staff. The EUROCONTROL Conops and Specification and the outline system description derived from it were the basis for the analysis. The analysis is not claimed to be complete, but all the main hazards at ATM system level and STCA component level are addressed.

5.7.3 Scope of System Considered for FHA

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].

GUIDANCE: 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. The situation is illustrated in Figure 5-5 below. Three boundary levels were considered:

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

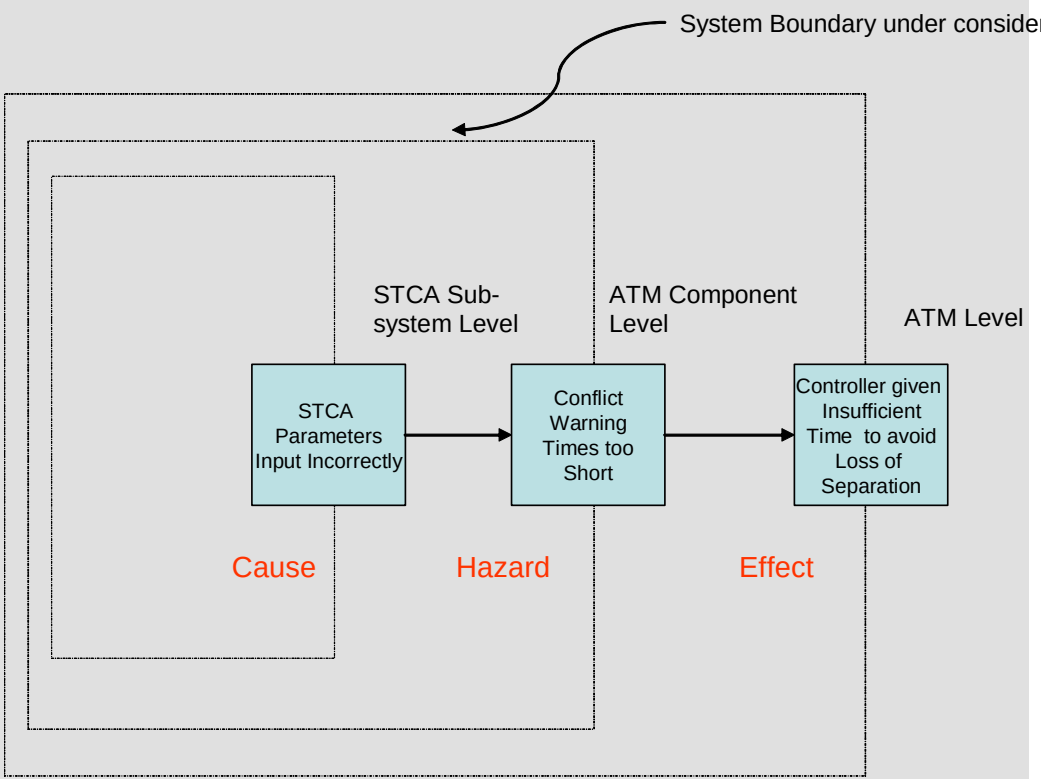


Figure 5-5: Hazards at boundary of System under assessment

5.7.4 Process

The STCA functions specified in the EUROCONTROL Specification 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 and Engineering staff by each ANSP. Controller 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 5.7.5 below.

5.7.5 FHA Results

The FHA results are set out in Table B1-5a. Each of the hazards identified at the ATM Component boundary was assessed for effect on ATM. The severity of the effects was not assessed as this is a matter for ANSPs to determine in the context of their own ATM system. Refer to EATM SAM FHA Guidance Material D[10] on how to do this. Safety Objectives have been expressed in

[10] EUROCONTROL Safety Assessment Methodology - SAM

terms of probability although no values have been assigned (left as To Be Determined (TBD) in Table B1-5a as this is a matter for ANSPs to address.

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, 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.

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. NOTE that the FHA may define other local requirements that are not covered in the specification.

Hazard Ref: **[Req. Ref]**	**Hazard – Defined at ATM Component Level**	**Hazard Effect on ATM**	**Severity and Exposure Time** ***(ANSPS to determine severity by Ref to SAM Severity Classification Scheme)***	**Mitigation or ATS System factors**	**Safety Objectives**
HA 1 [STCA-07] [STCA-08] [STCA-09] [STCA-13]	STCA alert warnings are not provided to the relevant controllers.	There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	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 should be made aware of loss of STCA as soon as possible. Radar tracks representation extended to highlight potential conflicts? Need to reinforce with a procedure for the provision of temporary alternative(s) to STCA	**SO1**: The probability of total loss of STCA shall be no greater than *TBD* *(See SAM FHA Guidance for the right form of words for expressing a safety objective)*
HA2 [STCA-07] [STCA-08] [STCA-09] [STCA-12] [STCA-13]	STCA does not reliably capture and direct controller attention to potentially conflicts	The Controller may not become aware of potential conflicts. There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Comprehensive Training and clear STCA policy	**SO2**: The probability of impaired functionality affecting the reliability of STCA shall be no greater than *TBD*
HA3	The Controller does not react effectively to resolve a conflict detected by STCA.	There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Comprehensive Training and clear STCA policy	**SO3**: The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be *TBD (e.g. reduced as far as reasonably practicable by training)*
HA4 [STCA-10] [STCA-11]	The number of Nuisance Alerts and possible False Alerts (credible corruption) are above an acceptable level	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	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	**SO4**: The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than *TBD* *See SAM FHA Guidance for the right form of words for expressing a safety objective)*

Table B1-5a: STCA Functional Hazard Analysis

5.7.6 Safety Objectives

The Safety Objectives[11] are derived from the FHA and are summarised in the Table B1-5b below. These will be decomposed to component-level safety requirements during the design phase PSSA. Each Safety Objective is given a unique identifier (SO1, SO2, etc) and a reference to the hazard (Haz HA1, Haz HA2, etc.) 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. The severity of the hazard effects have not been classified as this is for the ANSP to determine for their own ATM system. Also, the Safety Objectives are incomplete as no probability has been assigned; see SAM FHA for guidance on how to do this. ANSPs may take issue with assignment a probability to controller action as in S0 3. However, the idea is that the likelihood of a controller not carrying out an action effectively should be reduced as far as reasonably practicable - e.g. through training, effective HMI etc. The probability does not have to be expressed in quantitative terms.

SO Ref (Hazard Ref:)	STCA Safety Objectives
SO 1 (Haz. HA 1)	The probability of total loss of STCA shall be no greater than *TBD*.
SO 2 (Haz. HA 2)	The probability of impaired functionality affecting the reliability of STCA shall be no greater than *TBD*
SO 3 (Haz. HA 3)	The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be *TBD*
SO 4 (Haz. HA 4)	The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than *TBD*

Table B1-5b: Safety Objectives

5.7.7 Hazard Causes

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

GUIDANCE: Note that the objective here is to determine if there is any safety requirements for STCA in addition to those defined in the specification.

[11] Safety Objectives (SO) are qualitative or quantitative statements that define the maximum frequency at which a hazard can be accepted. Refer to SAM: Methods for setting safety objectives.

This activity corresponds to the PSSA process described in SAM. Essential pre-requisites for conducting a PSSA include a description of the system, 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 list of hazards and safety objectives comes primarily from FHA and is further completed during the PSSA. [Ref: SAM]

The hazard causes were identified with the aid of Fault Tree Analysis (FTA) and the results are shown on Figure 5-6. The top event in the Fault Tree – "*ATM safety will not be enhanced by STCA"* - was selected as the likely outcome of the occurrence of the hazards identified in the FHA.

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 Figure 5-6 is re-usable.

5.7.8 Fault Tree Analysis Boundary

The hazard causes are identified at ATM component level - see Figure 5-6; although some are identified at STCA sub-system level to provide an insight into specific areas for which assurance evidence will be required. The hazard identifier e.g. HA1 is included.

GUIDANCE: The conventional way of showing fault trees is top down, and formal software tools are available for this purpose. In the example which follows the fault tree is 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 STCA subsystem 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.

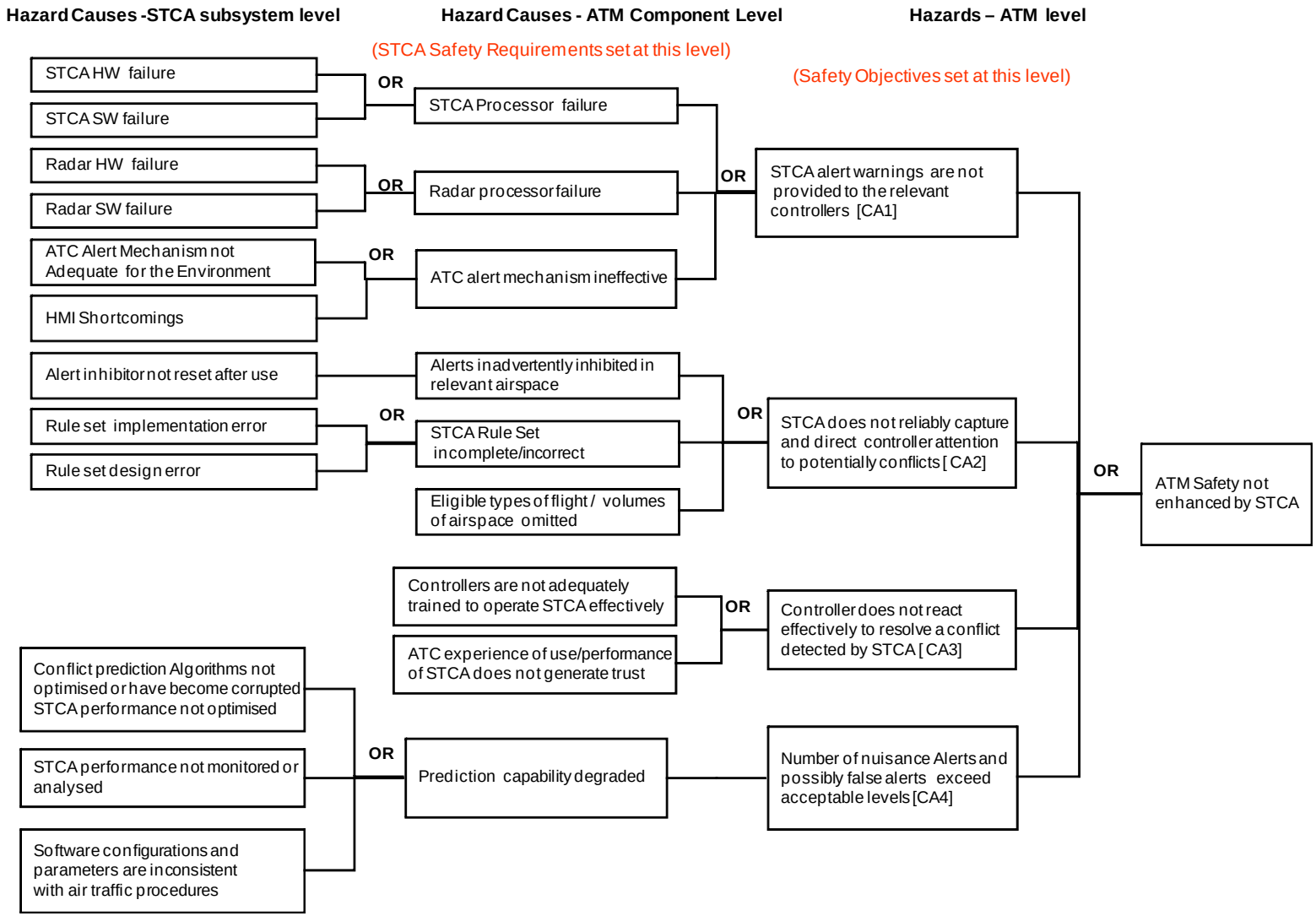


Figure 5-6: Fault Tree for ATM safety not enhanced by STCA

5.7.9 STCA Safety Requirements

STCA Safety Requirements[12] are derived from the Fault Tree. It is necessary to meet these in order to satisfy the Safety Objectives. These are included in the tables below. Some of these requirements are additional to those defined in the specification – for example process requirements for the development of software.

GUIDANCE: The safety requirements shown in the tables below are derived from the results of the FHA and the Fault Tree Analysis carried out above. The technical safety requirements relate more to STCA availability and operation and ANSPs will have to define the reliability and availability they wish to assign to these, consistent with their safety objectives. The procedure safety requirements relate to the mitigation actions from the FHA. ANSPs are likely to have to change the safety requirements stated below based on their own specifications and hazard analysis results.

5.7.10 Technical Safety Requirements

TSL 1 (HA 1)	The probability of the STCA Processor failing shall be not exceed To Be Determined (*TBD)*
TSL 2 (HA 1)	The probability of the Radar Processor failing shall be not exceed *TBD*
TSL 3 (HA 1)	The probability that the HMI for the automatic Alerting mechanism is not capable of Alerting controllers in the operational environment shall be *TBD* (e.g. reduced as far as reasonably practicable)
TSL 4 (HA 2)	All the data sets shall be validated for completeness and correctness in the relevant airspace and installed correctly *TBD*
TSL 5 (HA 2)	The probability that the Alert inhibition process compromises the STCA function shall be *TBD*
TSL6 (HA 3)	The probability that STCA parameters are incorrect shall be *TBD*
TSL 7 (HA 4)	The probability that STCA performance is not monitored or analysed shall be shall be *TBD*
TSL 8 (HA 4)	The probability that conflict prediction algorithms are not optimised or have become corrupted shall be *TBD*
TSL 9 (HA 4)	The probability that software configurations are inconsistent with air traffic procedures shall be *TBD*.

Table B1-5c Technical Safety Requirements

[12] Safety Requirements are derived from Safety Objectives. Generally, they specify the potential means to mitigate hazards i.e. to prevent occurrence of hazards or reduce the severity of their consequences. Refer to SAM Guidance Material A: Safety Requirements

5.7.11 Procedure Safety Requirements

PSL 1 (HA 1)	ATC procedures shall state what Controllers should do in the event of loss of an automatic alerting facility such as STCA.
PSL 2 (HA 2)	Procedures shall be put in place to ensure that the Controller is advised of any system changes which might degrade the performance of STCA
PSL 3 (HA 4)	The action to be taken when the number of nuisance Alerts is above acceptable limits shall be addressed in local instructions/regulations.

Table B1-5d: Procedure Safety Requirements

5.7.12 People Safety Requirements

PSL 1 (HA 3)	Controllers shall be adequately trained and competent so that the safety benefits of STCA can be realised operationally.

Table B1-5e: People Safety Requirements

5.8 That which is specified is realistic [Arg 1.6]

The assurance issue here is to verify and validate the requirements with a view to determining the required integrity for the system elements concerned. This is only feasible if the requirements are realistic.

Arg 1.6 - Assurance Objectives	Evidence Summary
(1) Show that the all hazard related aspects of the STCA design have been captured as Safety Requirements or (where applicable) as Assumptions	The safety requirements derived are totally consistent with the EUROCONTROL Specification. This is already claimed to be realistic as it is based on the practical experience of the SPIN Task Force/Sub-Group. No new Functional or performance requirements were identified via the FHA and FTA processes. Verified by comparison with the EUROCONTROL Specification.
(2) Show that the all the safety requirements are verifiable – i.e. satisfaction can be demonstrated by direct means (e.g. testing) or (where applicable) indirectly through appropriate assurance processes.	Judged to be true by review of the requirements, but ANSPs have to assign the integrity requirement.
(3) Show that the all the safety requirements are capable of being satisfied in a typical implementation in hardware, software, people and procedures.	The requirements are already implemented in real STCA systems to a greater or lesser extent as determined by the SPIN Task Force.
(4) Show that the all assumptions have been shown to be valid.	Issue for ANSP to address

Table B1-6: Assurance objectives to satisfy Arg 1.6

5.9 The evidence for the safety specification is trustworthy [Arg 1.7]

The Assurance issue is to provide backing evidence that the evidence supporting the arguments 1.1 to 1.6 is trustworthy.

Arg 1.7 - Assurance Objectives	Evidence Summary
(1) Confirm that the assurance processes , tools and techniques used were adequate for the task	*ANSP to supply details* Ref: Safety Plan
(2) Confirm that the competence of the people using them was adequate for the task	*ANSP to supply details*

Table B1-7: Assurance objectives to satisfy Arg 1.7

6. STCA COMPLIANCE WITH THE SAFETY REQUIREMENTS

6.1 Assurance Evidence

Evidence is required from the System Implementation and Integration phase to demonstrate that STCA has been implemented in accordance with the specification and that the transition to operational service will be acceptably safe i.e. that **Arg 2** and **Arg 3** can be considered to be true.

GUIDANCE: During this lifecycle phase the detailed design for all aspects of the system is completed (i.e. including people, procedures and equipment), and the system is developed and integrated into the ATM system. Any hazards arising from the planned transfer of the system to operation are identified and appropriate mitigation put in place. All the resources necessary to operate the system are in place.

Assurance evidence from this phase is beyond the strict scope of this Outline Safety Case; actual design assurance will depend entirely on the actual architecture and design adopted by each ANSP. The following parts of this document provide an outline only of the framework for the rest of the safety case.

6.2 STCA has been implemented in accordance with the specification [Arg 2]

The overall assurance objective is to show that the system implements the functional, non-functional and safety requirements relating to equipment, people and procedures correctly and completely.

6.2.1 Strategy

The strategy is to show that all functional, non-functional and safety requirements have been translated into design requirements and implemented successfully. This requires that evidence is available to satisfy the sub arguments 2.1 to 2.4 as shown in Diagram B2 below. Each of these is considered here, but to a very limited extent only given the scope of the Outline Safety Case.

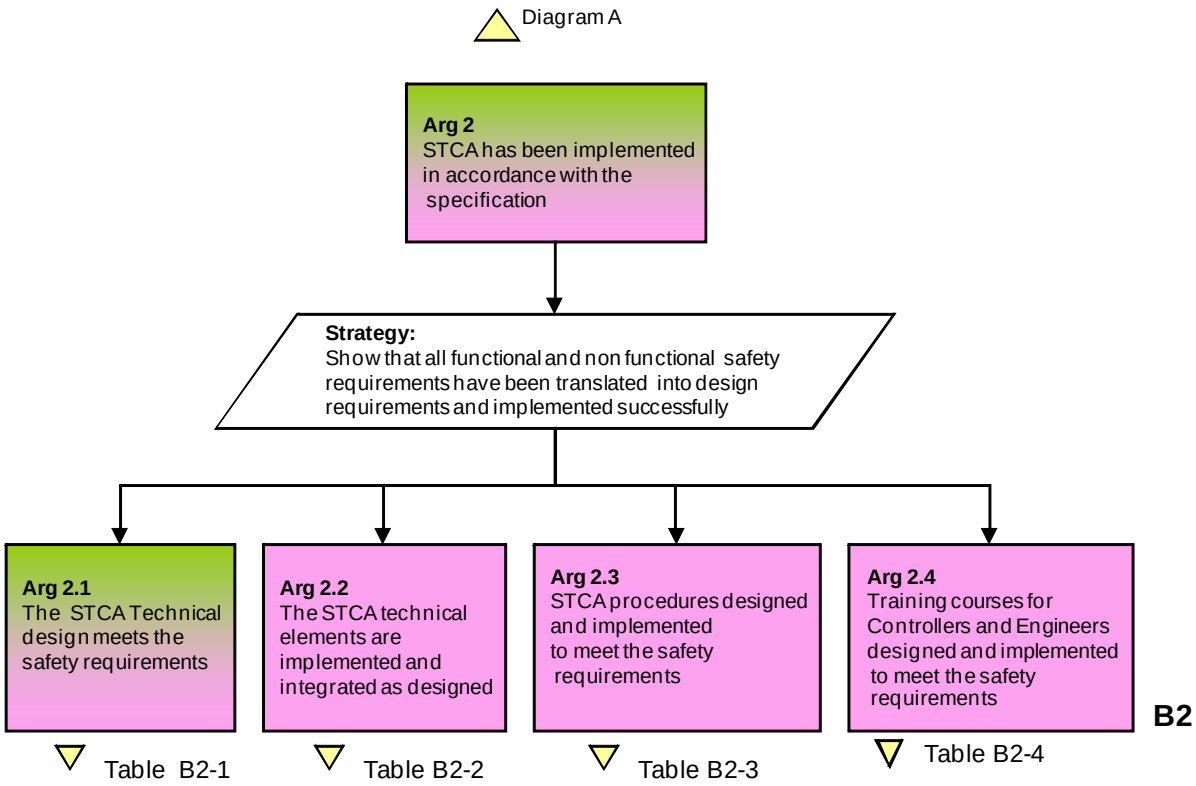


Diagram B2: System Implementation and integration Argument

6.3 The Technical System is designed to meet the safety requirements [Arg 2.1]

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 and 7.2.2]

Arg 2.1 - Assurance Objectives	Evidence Summary
(1) Confirm that the design requirements interpret the specification completely and correctly.	*Results of review of the design documents*
(2) Confirm that the design is documented and under configuration control	*ANSPs to identify design documents, and issue reference – to be referenced in the safety case.*
(3) Confirm that the design incorporates all the requirements, completely and correctly,	*ANSPs to provide a brief explanation of how this has been verified*

Table B2-1: Assurance Objectives to Satisfy Arg 2.1

6.4 The Technical System is implemented and integrated as designed [Arg 2.2]

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 7.2.2]

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

Arg 2.2 - Assurance Objectives	Evidence Summary
(1) Confirm that the system meets the specified functional and performance safety requirements.	*Consider each of the safety requirements in turn and provide evidence that they have been met.* See list of assurance activities in the Safety Plan Chap 7.2.2.

Table B2-2: Assurance Objectives to Satisfy Arg 2.2

6.4.1 Functional and non-functional requirements: Design Assurance

The functional and non-functional requirements from the EUROCONTROL STCA Specification are listed here. Evidence is to be supplied by ANSPs as outlined in italics.

STCA 01 - Policy:

The ANSP ***shall*** have a formal policy on the use of STCA consistent with the operational concept and safety management system applied to avoid ambiguity about the role and use of STCA.

Provide details of STCA Policy here, the organisational arrangements for managing STCA to make effective use of the system in achieving the maximum safety benefit.

STCA 02 - Responsibility for Management of STCA:

The ANSP ***shall*** assign to one or more staff, as appropriate, the responsibility for overall management of STCA.

GUIDANCE: The following Guidance information from the EUROCONTROL Guidance Material for STCA Appendix A[13] is adopted here with the following words which address the issue: *Despite that fact that developing an STCA may appear as a purely technical exercise, it is of paramount importance that the system is fit for the purposes of the specific operational context and consistent with the safety policy established inside the ANSP. In all ANSP organisations an adequate flow of information between engineering and operational staff is constantly required, especially in the tuning and validation phases.*

Provide details of the arrangements.

STCA 03 – Training and Competence:

The ANSP ***shall*** ensure that all controllers concerned are given specific STCA training and are assessed as competent for the use of the relevant to the STCA system.

[13] EUROCONTROL Guidance Material for STCA – Appendix A: Reference System

Provide details of the training designed and provided for controllers and engineers to operate and maintain the STCA system. Identify the training courses developed, and confirm that the required staff members have successfully completed those courses.

STCA 04-Requirements on Procedures:

Local instructions concerning use of STCA ***shall*** specify, *inter alia*:

a) the types of flight (GAT/OAT, IFR/VFR, RVSM/NON-RVSM, etc.) which are eligible for generation of alerts;

b) the volumes of airspace within which STCA is implemented;

c) the method of displaying the STCA to the controller;

d) in general terms, the parameters for generation of alerts as well as alert warning time;

e) the volumes of airspace within which STCA can be selectively inhibited and the conditions under which this will be permitted;

f) conditions under which specific alerts may be inhibited for individual flights; and

g) procedures applicable in respect of volumes of airspace or flights for which STCA or specific alerts have been inhibited.

Describe here the specific type of operation for which this system is intended and the specific volume of airspace and type of airspace where the STCA is to be used.

STCA 05 - Requirement on Controller Actions:

In the event an alert is generated in respect of controlled flights, 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.

Provide here a brief outline of the procedure and identify where it is documented

STCA 06- Requirement on Performance Analysis:

STCA performance ***shall*** be analysed regularly to identify possible shortcomings related to STCA.

Provide here a brief outline of the procedure and identify where it is documented. Reversionary procedures may also need to be defined for those circumstances where STCA is not performing correctly.

STCA 07- Alerting Performance:

STCA ***shall*** detect and alert operationally relevant conflicts involving at least one eligible aircraft.

Provide a brief description of how this is done.

STCA 08 –Alerting performance:

STCA ***shall*** provide alerts for operationally relevant conflicts.

Provide a brief description of how this is done.

STCA 09 - Alerting Performance:

STCA alerts ***shall*** attract the controller's attention and identify the aircraft involved in the conflict; STCA alerts ***shall*** be at least visual.

Provide a brief description of how this is done.

STCA 10- Alerting Performance:

The number of nuisance alerts produced by STCA ***shall*** be kept to an effective minimum.

Provide a brief description of how this is done.

STCA 11- Alerting Performance:

The number of false alerts produced by STCA ***shall*** be kept to an effective minimum.

Provide a brief description of how this is done.

STCA 12- Warning Time:

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.

Provide a brief description of how this is done.

STCA 13- Warning Time:

STCA ***shall*** continue to provide alert(s) as long as the alert conditions exist.

Provide a brief description of how this is done.

STCA 14 - Alert Inhibition:

STCA ***shall*** provide the possibility to inhibit alerts for predefined volumes of airspace and for individual flights.

Provide a brief description of how this is done.

STCA 15- Alert Inhibition:

Alert inhibitions ***shall*** be made known to all controllers concerned.

Provide a brief description of how this is done.

STCA 16- Status Information:

Status information ***shall*** be presented to supervisor and controller working positions in case STCA is not available.

Provide a brief description of how this is done.

STCA 17 - Data Recording:

All pertinent STCA data ***shall*** be made available for off-line analysis.

Provide a brief description of how this is done.

6.4.2 Technical System Safety Requirements: Design Assurance

The safety requirements derived from the PSSA are listed here. Evidence is to be supplied by ANSPs as outlined in italics. Refer to the Safety Plan 7.2.2 for information on the tools and techniques that may be relied on for assurance purposes.

TSL 1 (HA 1) The probability of the STCA Processor failing shall be not exceed *TBD*

Provide evidence that the system reliability is likely to achieve this Safety Requirement

TSL 2 (HA 1) The probability of the Radar Processor failing shall be not exceed *TBD*

Provide evidence that the system reliability is likely to achieve this Safety Requirement

TSL 3 (HA 1) The probability that the HMI for the automatic Alerting mechanism is not capable of Alerting controllers in the operational environment shall be *TBD* (e.g. reduced as far as reasonably practicable)

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 4 (HA 2) All the data sets shall be validated for completeness and correctness in the relevant airspace and installed correctly *TBD*

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 5 (HA 2) The probability that the Alert inhibition process compromises the STCA function shall be *TBD*

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 6 (HA 3) The probability that STCA parameters are incorrect shall be *TBD*

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 7 (HA 4) The probability that STCA performance is not monitored or analysed shall be shall be *TBD*

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 8 (HA 4) The probability that conflict prediction algorithms are not optimised or have become corrupted shall be *TBD*

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

TSL 9 (HA 4) The probability that software configurations are inconsistent with air traffic procedures shall be *TBD*.

Explain why it is claimed that the system will meet this Safety Requirement. Describe the assurance carried out to demonstrate it.

6.5 STCA Procedures Designed and Implemented to Meet the Requirements [Arg 2.3]

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.

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 7.2.3].

Arg 2.3 - Assurance Objectives	Evidence Summary
(1) Confirm that procedures have been designed to meet the safety requirements	*Consider each of the safety requirements in turn and provide evidence that they have been met.* See the illustrative example below. See [Safety Plan 7.2.3]
(2) Confirm that the procedures have been implemented.	*Provide evidence that this has been done*

Table B2-3: Assurance Objectives to Satisfy Arg 2.3

6.5.1 Procedure Safety Requirements

The safety requirements derived from the PSSA are listed here. Evidence is to be supplied by ANSPs as outlined in italics. [Safety Plan 7.2.3].

PSL 1 (HA 1) ATC procedures shall state what Controllers should do in the event of loss of an automatic alerting facility such as STCA.

Explain why it is believed that this Safety Requirement is met. Describe the arrangements in place to achieve it.

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.

PSL 2 (HA 2) Procedures shall be put in place to ensure that the Controller is advised of any system changes which might degrade the performance of STCA

Explain why it is believed that this Safety Requirement is met. Describe the arrangements in place to achieve it.

PSL 3 (HA 4) The action to be taken when the number of nuisance Alerts is deemed to be excessive shall be addressed in local instructions/regulations.

Explain why it is believed that this Safety Requirement is met. Describe the arrangements in place to achieve it.

6.6 Training Courses for Controllers and Engineers designed and implemented to meet the requirements [Arg 2.4]

The safety requirements derived from the PSSA are listed here. Evidence is to be supplied by ANSPs as outlined in italics [Safety Plan 7.2.4].

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, and that staff have successfully completed those courses.

Arg 2.4 - Assurance Objectives	Evidence Summary
(1) Confirm that the training courses have been designed to meet the requirements	*Consider each of the safety requirements in turn and provide evidence that they have been met.* See [Safety Plan 7.2.4]
(2) Confirm that the training courses have been implemented.	*Provide evidence that this has been done*

Table B2-4: Assurance Objectives to Satisfy Arg 2.4

6.6.1 People Safety Requirements

PSL 1 (HA 3) Controllers shall be adequately trained and competent so that the safety benefits of STCA can be realised operationally.

Explain why it is believed that this Safety Requirement is met. Describe the arrangements in place to achieve it.

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.

6.7 Transition to Operational Service of the STCA system will be acceptably Safe [Arg 3]

6.7.1 Assurance Evidence

The overall assurance objective is to show that the existing ATM system will not be put at risk during the transition to operation of the STCA system and that all the resources necessary for the safe operation of the system are in place – people, procedures and equipment. This requires that evidence is available to satisfy the Sub Arguments 3.1 to 3.3 as shown in Diagram B3 below. Each of these is considered here, but to a very limited extent only given the scope of the Outline Safety Case.

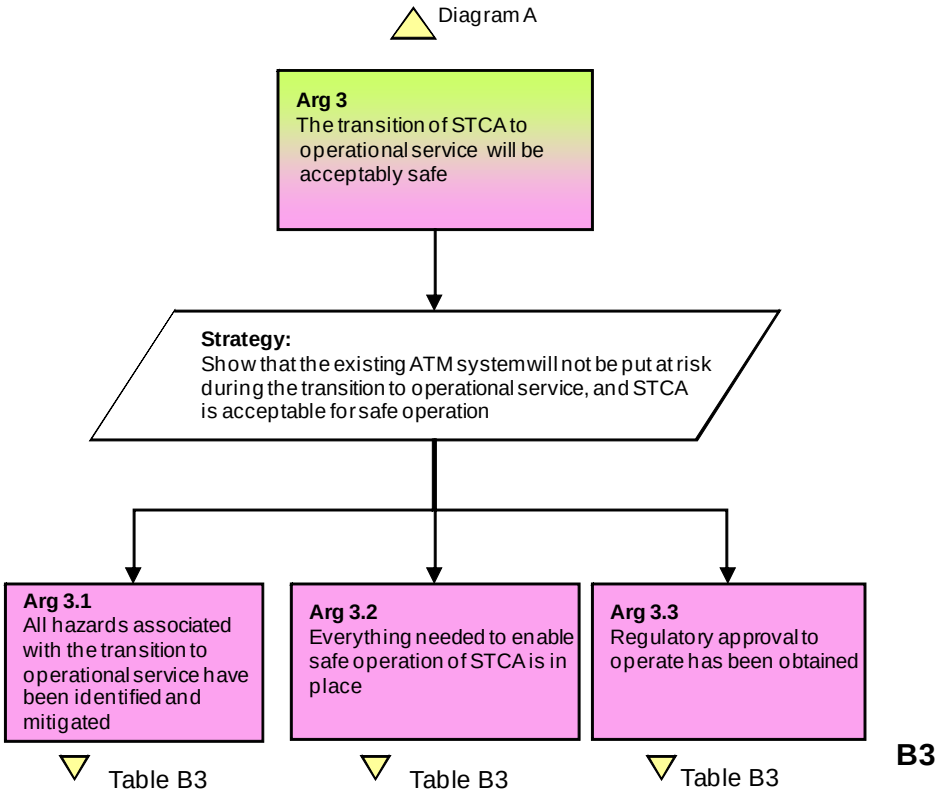


Diagram B3: Safe Transition to Operational Service

Arg 3 - Assurance Objectives	Evidence Summary
(1) Show that safety requirements for the transfer to operation have been specified	*Describe the steps take to ensure that existing ATM system will not be put at risk during the transition to operation of the STCA system.* See Safety Plan activities 7.3.1 and illustrative example below.
(2) Confirm that the system reliability and integrity accepted as meeting the functional and performance safety requirements.	*Include here a summary results of functional tests carried out during commissioning, in so far as they address safety.*
(3) Confirm that the HF and HMI accepted as satisfactory	*Provide summary of the evidence confirming acceptability and how it was demonstrated.*
(4) Confirm that the sufficient trained staff available to operate and maintain the system.	*Provide evidence that all the resources necessary for the safe operation of the system are in place – people, procedures and equipment.*
(5) Confirm that the procedures are published and promulgated to all relevant staff. These should include procedures for switch over to operational service, and any associated contingency.	*Provide summary of the evidence confirming this.*
(6) Confirm that the operational validation trials satisfactory	*Provide summary of the evidence confirming this.*
(7) Confirm that the system shortcomings highlighted and accepted for operation.	*Provide summary of the evidence confirming this.*
(8) Confirm that the regulatory approval to operate obtained.	*Provide summary of the evidence confirming this.*

Table B3: Assurance objectives to satisfy Arg 3

6.7.2 Safety Requirements for the Transfer to Operations Specified [Arg 3.1]

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 STCA - 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 ATM 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].

7. SYSTEM OPERATION AND MAINTENANCE

7.1 The Safety of STCA will continue to be demonstrated in operational service (Arg 4)

7.1.1 Assurance Evidence

The assurance issue is to ensure that STCA is maintained and operated consistent with the requirements of Criteria 01.02 and 03. This requires that its performance is optimised for all areas of application [Safety Plan 7.4.1].

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.

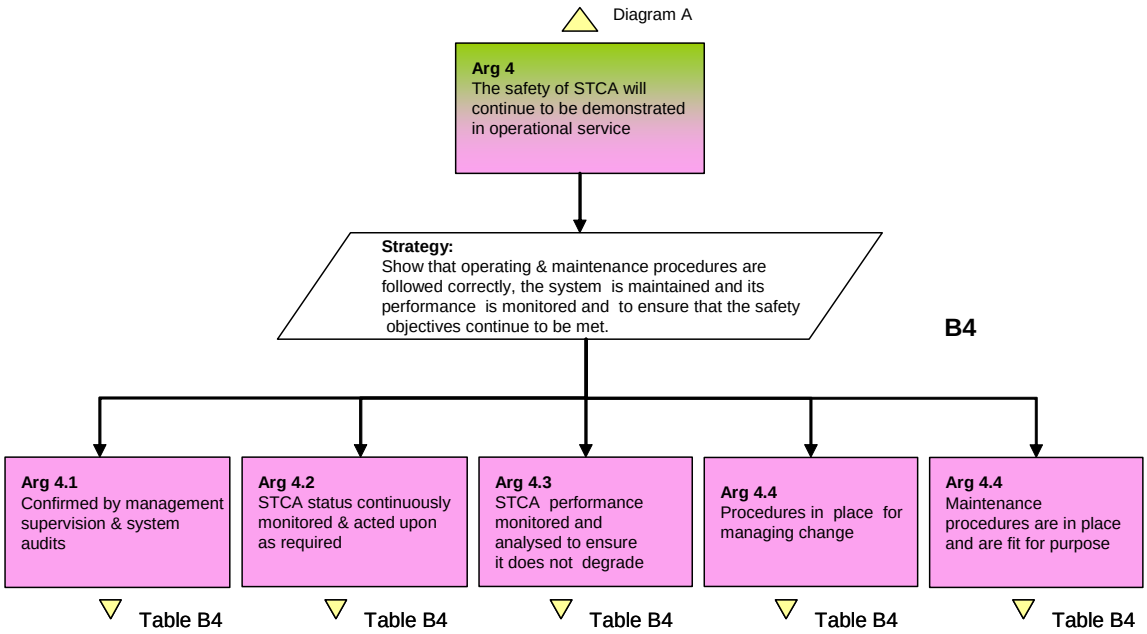


Diagram B4: Safety in Operational Service

Arg 4 – Assurance Objectives	Evidence Summary
(1) Confirm that the Staff have been assigned with the responsibility for management of STCA (to fulfil the above functions)	*Provide summary of the evidence*
(2) Confirm that the a formal process exists for monitoring STCA Status	*Provide summary of the evidence*
(3) Confirm that the a formal process exists for monitoring STCA and analysing the results	*Provide summary of the evidence*
(4) Show that the system remains optimised for its role and keeps pace with changing operational requirements	*Provide summary of the evidence*
(5) Show that ATC are advised of any system changes that might affect the safety performance	*Provide summary of the evidence*
(6) Show that maintenance procedures are in place and are fit for purpose	*Provide summary of the evidence*

Table B4: Assurance objectives to satisfy Arg 4

8. CONCLUSIONS

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.

GUIDANCE: Further guidance on Safety Case conclusions can be found in the EUROCONTROL SCDM [Ref 8].

8.1 Assumptions

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).

8.2 Limitations and shortcomings

GUIDANCE: Include here any design or operational shortcomings or limitations, including any identified through the testing, installation and integration into the Air Traffic Service.

8.2.1 Shortcomings

List here 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.

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

8.2.2 Limitations

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.

8.3 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.

9. LIST OF ABBREVIATIONS

ANSP	Air Navigation Service Provider
Conops	Concept of operation
ECIP	European Convergence and Implementation Plan
ENPRM	EUROCONTROL Notice of Proposed Rule-Making
ESP	European safety Programme
ESARR	EUROCONTROL Safety Regulatory Requirements
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
GSN	Goal-Structuring Notation
HF	Human Factors
HMI	Human Machine Interface
NSA	National Supervisory Authority
PSSA	Preliminary Safety Assessment Process
SAM	Safety Assessment Methodology
SCDM	Safety Case Development Manual
SPIN	Safety nets: Planning Implementation and eNhancements (Task Force)
SPIN	Safety nets Performance Improvement Network (Sub Group)
SRC	Safety Regulation Commission
SSA	System Safety Assessment
STCA	Short Term Conflict Alert
TBD	To Be Determined

10. REFERENCES

1. EUROCONTROL Specification for Short Term Conflict Alert
2. EUROCONTROL Guidance Material for Short Term Conflict Alert
3. EUROCONTROL Guidance Material for Short Term Conflict Alert Appendix A: Reference System
4. Safety Assessment Made Easier Version 0.92
5. SRC Action paper SRC28/06. SRC Policy on Ground Based Safety Nets
6. SPIN: Survey of Practices in Safety Nets; Summary report Edition 1.01
7. SCDM: EUROCONTROL Safety Case Development Manual, Edition 2.2
8. EUROCONTROL ESARR 4 – Risk Assessment and Mitigation, Edition 1.0

END OF DOCUMENT