EUROCONTROL

EUROCONTROL Guidance Material for Short Term Conflict Alert
Appendix B-2: Generic Safety Plan for STCA Implementation

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

EUROCONTROL

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidance Material for Short Term Conflict Alert **Appendix B-2: Generic Safety Plan for STCA Implementation**		
	ALDA Reference:	06/12/14-23
Document Identifier	**Edition Number:**	1.0
	Edition Date:	14 December 2006

Abstract

This document is the second 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 contains a generic Safety Plan.

Keywords

Safety Nets
STCA
Safety Argument
Safety Plan
Safety Case

Contact Person(s)	Tel	Unit
Ben Bakker	+32 2 72 91346	DAP/ATS

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

ELECTRONIC SOURCE		
Path:	\\HHBRUNA02\bakkerb$\STCA	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	370 Kb

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

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

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Technical Manager	B. Bakker	14.12.06
ATC Domain Manager	M. Griffin	18.12.06
ESP Programme Manager	T. Licu	18.12.06
Head of DAP/ATS	P. Dias	18/12/06
Head of DAP/SSH	A. Skoniezki	18/12/2006
Deputy Director ATM Programmes	E. Merckx	18/12/2006

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	17-5-2005		Draft for review by SPIN Task Force	All
0.2	10-8-2006		Results from review incorporated; status raised to proposed issue	All
1.0	14-12-2006	06/12/14-23	Formatting changes	All

CONTENTS

EXECUTIVE SUMMARY

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

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

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

The documented assurance should contain the evidence, arguments and assumptions as to why a system is safe to deploy. The process of developing and acquiring the necessary safety assurance is considerably enhanced if the activities to obtain it are planned from the outset, ideally during the system definition phase of a project, and documented in a safety plan.

This document is a generic safety plan for STCA implementation, covering all the system lifecycle phases. It describes what activities should be considered at each phase, who should do them, and what the criteria for success are. The output of the activities in the safety plan should provide the evidence necessary to complete the safety case

Another advantage of having a safety plan is that it can be offered to the NSA in order to get an early indication of the likelihood that the planned assurance activities will lead to NSA approval of the system.

Although the activities scheduled in a safety plan may be regarded as part of a project plan, it is advantageous for safety management purposes to keep it as separate document. Note that not all the assurance activities will be known at the outset and the safety plan may need to be updated as system development progresses.

1. INTRODUCTION

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

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

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

The set of documents consists of:

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

It is assumed that the Safety Assurance – i.e. arguments, evidence and assumptions - that STCA is safe for deployment in operation will be recorded in each ANSP's Safety Case.

In order to facilitate the ANSPs' safety work, this Safety Plan, an accompanying Safety Argument and an Outline Safety Case have been developed by EUROCONTROL to substantiate, as far as possible at this stage, the claim that STCA will provide a substantive safety benefit in ATM operations.

2. AIM

This Safety Plan is intended as guidance to ANSPs on planning the safety assurance activities, collecting the evidence required to support the safety argument and ensuring that adequate safety assurance documentation will be produced in a timely manner. The Plan should be read with reference to the Safety Argument, and the Outline Safety Case should be adapted / developed by ANSPs to suit their own particular implementation of STCA.

3. PURPOSE

The purpose of this Safety Plan is to detail the activities which are necessary to provide safety assurance and how they are to be discharged. It identifies who undertakes these activities; the outputs from the activities; the criteria for success and the tools, techniques, methods or standards to be used.

4. SCOPE

This Plan identifies the safety activities that should be undertaken in the definition, development and deployment of an STCA system. The scope of this document encompasses all phases of a system lifecycle and all system elements (people, procedures and equipment.

5. ROLES AND RESPONSIBILITIES

Four main roles and responsibilities are identified under the acronym **LDCI:**

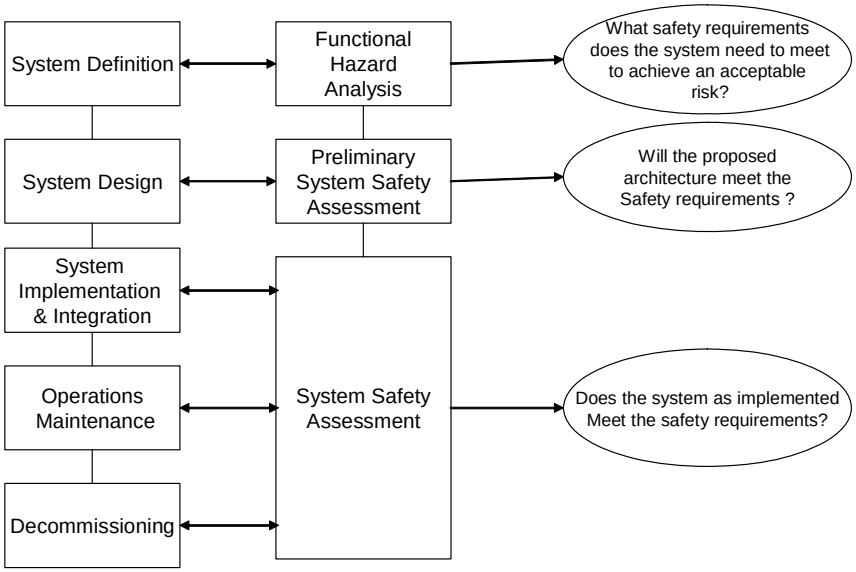
Role	Responsibility
Lead:	Responsible for ensuring the assurance and evidence is provided
Do:	Responsible for providing assurance and evidence
Consult:	Who should be consulted in the process
Inform:	Who should be informed of the outcome

Note: it is accepted that there may not be staff posts with the titles used in the tables presented in section 7 below, but it is assumed that someone will perform the role. ANSPs will need to tailor the roles to their organisation when instantiating this Plan.

6. SYSTEM LIFECYCLE PHASES

6.1 Safety Activities during System Lifecycle

The following Figure from the EUROCONTROL SAM is used to illustrate the relationship between the safety assessment activities referred to in this Plan and the system lifecycle:



6.2 System Definition

The basic operational objectives for the system are established during the system definition phase. The concept of operations is developed and the feasibility of implementing it in the existing ATM system is determined.

The policy for STCA is determined. Assumptions about the system boundaries and its operational environment are recorded.

The functional and performance requirements to enable the concept are specified. These are subjected to Functional Hazard Assessment FHA and risk assessment to identify hazards that might impact on the design of the system. Safety objectives and high level safety requirements are derived for the system and mitigation for identified hazards determined.

Human factor issues are highlighted and training requirements are identified. ATC & Engineering procedures are specified.

The assurance activities are listed in Table 7.1 of the Assurance Strategy

Note: **Verification** in the context of this Plan is about establishing that an activity has be done as required; **Validation** is about confirming that it has been done completely and correctly. The abbreviation V&V is used throughout to indicate these processes.

6.3 System Design

The system architecture is determined which can reasonably be expected to achieve the functional and performance requirements and the safety objectives specified in the FHA. HR issues/hazards are mitigated or “designed out” where practical.

A preliminary system safety assessment is carried out to determine potential causes of hazards arising from the proposed system design. The resulting safety requirements have to be achieved by the design.

The technical design should comply with the specification, safety requirements and any regulatory requirements.

Training courses are designed. ATC & Engineering procedures are developed.

The assurance activities are listed in Table 7.2 of the Assurance Strategy

6.4 System Implementation & Integration

The Technical system is developed and implemented in hardware and software. The system elements should meet the safety requirements and be able to meet the safety objectives.

Any hazards to the existing ATM system arising from integration have been identified and addressed.

Training courses are established and running. ATC & Engineering procedures are integrated into ANSP documentation.

Arrangements are in place for management and control of changes to ensure that any new hazards introduced are identified and assessed.

The assurance activities are listed in Table 7.3 of the Assurance Strategy.

6.5 Transfer to Operations

The system (people, procedures and equipment) is assessed as fit for purpose. All limitations and shortcomings are identified and addressed. An approved safety case is completed and is accepted by the ANSP and the regulator where necessary.

The assurance activities are listed in Table 7.4 of the Assurance Strategy.

6.6 Operation and Maintenance

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

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

The assurance activities are listed in Table 7.5 of the Assurance Strategy

7. STRATEGY FOR ASSURANCE

The following Tables contain details of the planned assurance activity against the specified requirements for STCA, the safety objectives and safety

requirements contained in the Outline Safety Case. The activities are scheduled according to the system lifecycle phases – a separate Table for each. Each activity is given a unique reference number e.g. [Ref 7.1.1] and the argument which it supports is identified e.g. Arg 1.1.

System Life Cycle Phase: System Definition		Ref: EUROCONTROL SAM FHA Guidance Material				
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.1.1 [Arg 0]	STCA will provide a substantive safety benefit in ATM operations	Show by comparison of ATM safety performance data with and without STCA Determine % of conflicts alerted with warning time of 30 seconds or more..	ATM safety performance data Results of analysis	X% of eligible conflicts alerted of which Y% have a warning time of 30 seconds or more.	L: ANSP Management D: ANSP Management C: Incident data base and other ANSPS I: Safety Manager	Documented safety performance data.
7.1.2 [Context 01]	Clear and unambiguous policy regarding use of STCA	Confirm by review that policy exists and that it is consistent with NSA regulatory requirements and EUROCONTROL specification	Written Policy Results from review	Published Policy endorsed by ANSP management and where necessary, the NSA Regulator.	L: ANSP Management D: ANSP Management C: NSAr I: Safety Manager	Documented and included in safety case
7.1.3 [Context 02]	Concept of operation, consistent with declared policy	Confirm by review that the concept of operation exists and that it is consistent ANSP policy for STCA. Confirm that it was developed in concert with operational staff and agreed with them	Written concept. Results from review	Documented concept of operation endorsed by ANSP management and where necessary, the NSA Regulator. No inconsistencies noted compared to policy.	L: ANSP Management D: ANSP Management C: NSA I: Safety Manager	Documented and included in safety case
7.1.4 [Arg 1.1]	Assumptions about system boundaries and operational environment defined	Confirm by review that assumptions are feasible for the planned system	Written assumptions Results from review	Documented assumptions confirmed by ATC and engineering as appropriate.	L: ANSP Management D: ANSP Management C: Operations Managers I: Safety Manager	Documented and included in safety case
7.1.5 [Arg 1.2]	STCA Functional & Performance requirements specified.	Confirm by review that the requirements are complete and correct, consistent with the concept of operation and compatible with the EUROCONTROL Specification.	Written specification Results from review Compliance Matrix	Compatible with EUROCONTROL Specification. Achievable.	L: ANSP Management D: ANSP Management C: Operations Managers & NSA I: Safety Manager	Documented and referenced in safety case
7.1.6 [Arg 1.3]	HMI requirements specified	Confirm by review that the requirements are feasible and compatible with the intended operational environment	Written requirements Review findings.	Acceptable to Controllers	L: ANSP Management D: ANSP Management C: HF Expert I: Safety Manager	Documented and referenced in safety case

TABLE 7.1 STRATEGY FOR ASSURANCE – SYSTEM DEFINITION

System Life Cycle Phase: System Definition Ref: EUROCONTROL SAM FHA Guidance Material						
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.1.7 [Arg 1.3]	STCA Training Requirements for Controllers & Engineers specified	Review of training Requirements	Written requirements Review findings.	Objectives defined correctly in relation to requirements. Training specification addresses objectives. Target audience defined. Training plan feasible.	L: ANSP Management D: ANSP Management C: ATC & Engineering I: Safety Manager	Documented and referenced in safety case
7.1.8 [Arg 1.3]	Requirements for STCA operating procedures specified	Review of procedure Requirements	Written requirements Review findings.	Requirements defined correctly in relation to STCA functional and performance requirements. Users defined.	L: ANSP Management D: ANSP Management C: ATC & Engineering I: Safety Manager	Documented and referenced in safety case
7.1.9 [Arg 2.2]	All hazards correctly identified and assessed	Confirm by review that Functional Hazard Assessment was formally completed	Documented results of FHA including system Safety Objectives and safety requirements hazard Mitigation	Criteria in SAM Evaluation Guidance for FHA Criteria in SAM Evaluation Guidance for PSSA	L: ANSP Management D: FHA Expert C: ATC Staff I: Safety Manager	Documented and included in safety case
7.1.10 [Arg 2.3]	STCA Safety Requirements specified	Preliminary System Safety Assessment formally completed	Documented results of PSSA including Safety Requirements	Criteria in SAM Evaluation Guidance for FHA Criteria in SAM Evaluation Guidance for PSSA	L: ANSP Management D: PSSA Expert C: ATC Staff I: Safety Manager	Documented and included in safety case
7.1.11 [Arg 4.2]	Requirements for procedures for monitoring and analysing STCA performance specified	Review of procedure Requirements	Written requirements Review findings.	Requirements defined correctly in relation to STCA functional and performance requirements. Users defined.	L: ANSP Management D: ANSP Management C: ATC & Engineering I: Safety Manager	Documented and referenced in safety case
7.1.12 [Arg 4.2]	Requirements for procedures for maintaining STCA specified	Review of procedure Requirements	Written requirements Review findings.	Requirements defined correctly in relation to STCA functional and performance requirements. Users defined.	L: ANSP Management D: ANSP Management C: ATC & Engineering I: Safety Manager	Documented and referenced in safety case

TABLE 7.1 (CONT) STRATEGY FOR ASSURANCE – SYSTEM DEFINITION

System Life Cycle Phase: System Design		Ref: EUROCONTROL SAM PSSA Guidance Material				
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.2.1 [Arg 3.1]	The STCA technical system is designed to meet the specified functional & performance requirements	Review of documented design to confirm completeness and correctness	Documented design under configuration control. Results of review	Accepted as complete and correct by ANSP.	**L**: ANSP Management D: ATC & Engineering C: Developer I: Safety Manager	Referenced in Safety Case
7.2.2 [Arg 3.1]	The STCA technical system is designed to meet the specified safety objectives and safety requirements	Review of documented design to confirm completeness and correctness	Documented design under configuration control. Results of review	Accepted as complete and correct by ANSP.	L: ANSP Management D: ANSP Management C: Developer I: Safety Manager	Referenced in Safety Case
7.2.3 [Arg 3.4]	STCA Training courses for Controllers & Engineers designed to meet specified safety requirements.	Review of documented Training courses to confirm completeness and correctness	Documented Training courses under configuration control Results of review	Accepted as consistent with training objectives by ANSP.	L: ANSP Management D: ANSP Management C: Training staff & HF Expert I: Safety Manager	Documented and referenced in safety case
7.2.4 [Arg 3.3]	Operating procedures developed as specified	Review of documented procedure to confirm completeness, correctness and suitability for use	Documented procedures under configuration control. Results of review	Accepted as meeting requirements by ANSP. Confirmed as suitable for use by HF expert	L: ANSP Management D: ANSP ATC & Eng C: HF Expert I: Safety Manager	Referenced in Safety Case
7.2.5 [Arg 3.3]	Procedures for performance monitoring and analyses developed as specified	Review of documented procedure to confirm completeness, correctness and suitability for use	Documented procedures under configuration control. Results of review	Accepted as meeting requirements by ANSP. Confirmed as suitable for use by HF expert	L: ANSP Management D: ANSP ATC & Eng C: HF Expert I: Safety Manager	Referenced in Safety Case
7.2.6 [Arg 3.3]	Procedures for maintaining STCA developed as specified.	Review of documented procedure to confirm completeness, correctness and suitability for use	Documented procedures under configuration control. Results of review	Accepted as meeting requirements by ANSP. Confirmed as suitable for use by HF expert	L: ANSP Management D: ANSP ATC & Eng C: HF Expert I: Safety Manager	Referenced in Safety Case

TABLE 7.2 STRATEGY FOR ASSURANCE – SYSTEM DESIGN

System Life Cycle Phase: System Implementation & Integration			Ref: EUROCONTROL SAM SSA Guidance Material			
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.3.1 [Arg 3.2]	The STCA technical system is implemented and integrated as designed.	HW & SW Reviews Reliability & Integrity Testing Performance analysis Operating Trials Accuracy analysis Task Analysis Simulation Trials	Documented analysis & test results Documented trial Results Documented simulation results Evidence of test coverage Evidence of low probability of residual faults (from analysis of the design process and product)	Functional & Performance requirements confirmed by results. ESARR 6 for SW	L: ANSP Management D: Developer C: ANSP ATC, Eng, HF experts & regulator I: Safety Manager	Results summarised in Safety Case
7.3.2 [Arg 3.4]	STCA Training courses for Controllers & Engineers implemented as designed.	Review of course schedule and feedback reports	Course Schedule List of attendees Documented results of review.	All staff trained to plan	L: ANSP Management D: ANSP Training Staff C: ATC & Engineering & HF Expert I: Safety Manager	Documented and referenced in safety case
7.3.3 [Arg 3.3]	STCA procedures implemented and integrated as designed	Establish by review that procedures have been included in ANSP ATC procedures, Operating and Maintenance Manuals and/or Documentation	ATC procedures manual, Operating and Maintenance Manuals Results of Review	All procedures documented and implemented to plan	L: ANSP Management D: ANSP Operations Managers C: Documentation Controller I: Safety Manager	Documented and referenced in safety case
7.3.4 [Arg 3.5	Safety Requirements for system integration and transfer into operation specified	Hazard Assessment of integration and transfer to operations process	Documented results of Hazard Assessment including Safety requirements for hazard mitigation	Safety requirements reflected in plans for system integration and transfer to operations	L: ANSP Management D: ANSP Expert C: ATC & Eng Staff I: Safety Manager	Documented and included in safety case

TABLE 7.3 STRATEGY FOR ASSURANCE – SYSTEM IMPLEMENTATION AND INTEGRATION

System Life Cycle Phase: Transfer to Operations						
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.4.1 [Arg 4.1]	Reliability & Integrity accepted as adequate for operation	Confirm by review of the results of system acceptance tests and commissioning process	Results of acceptance tests Commissioning procedure Results of review	Accepted as satisfactory by ANSP	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Summarised and referenced in the Safety Case
7.4.2 [Arg 4.1]	HF Issues addressed regarding introduction of STCA and HMI accepted by operational staff	Confirm by review of the HMI with operation staff and HF expert	Results of review	Accepted as satisfactory by controllers and HF expert	L: ANSP Operations D: ANSP Operations Manager C: HF Expert I: ANSP Manager	Summarised in the Safety Case
7.4.3 [Arg 4.1]	Policy promulgated to all relevant staff	Confirm by review of how this was done	Promulgation media Results of review	Demonstrably effective process	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Summarised in the Safety Case
7.4.4 [Arg 4.1]	Sufficient Staff trained and competent to operate and maintain the system	Confirm by review of the number of staff trained to schedule.	List of trained staff Results of review	Accepted by ANSP as sufficient for safe operation.	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Summarised in the Safety Case
7.4.5 [Arg 4.1]	Procedures published and promulgated to all relevant staff	Confirm by review of the distribution of published procedures	Published procedures Results of review	All relevant staff in receipt of procedures	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Summarised in the Safety Case

TABLE 7.4 STRATEGY FOR ASSURANCE – TRANSFER TO OPERATIONS

System Life Cycle Phase: Transfer to Operations						
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.4.6 [Arg 4.1]	Regulatory approval to operate obtained	Confirm that written approval was sought and received from NSA	Written approval	Accepted by NSA as compliant with NSA regulations	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Summarised in the Safety Case
7.4.7 [Arg 4.1]	Operational validation trials satisfactory	Confirm that the STCA system performed as required during trials in the operational environment	Documented Trials Review of results	Accepted by ANSP and NSA as sufficient for safe operation.		
7.4.7 [Arg 4.1]	System short comings highlighted and accepted for operation	Confirm shortcomings recorded with rationale for acceptance.	Documented shortcomings Rationale for acceptance written by ANSP	Accepted by ANSP as safe for operation.	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Completed and Signed Safety Case

TABLE 7.4 (CONT) STRATEGY FOR ASSURANCE – TRANSFER TO OPERATIONS

System Life Cycle Phase: System Operation & Maintenance						
Ref:	STCA Requirement	Assurance Activity	Evidence	Criteria for Success	Responsibility	Documentation
7.5.1 [Arg 4.2]	ATC advised of any system changes that might affect the performance of STCA	Establish that formal process exists and is documented and applied	Written procedure Confirmation of use	No adverse reports by ATC	L: ANSP Operations D: ANSP Eng Manager C: Safety Manager I: ANSP Manager	Procedure in Maintenance manuals
7.5.2 [Arg 4.2]	Alert inhibition restricted	Establish that formal process exists and is documented and applied	Written procedure Confirmation of use	No related incidents	L: ANSP Operations D: ANSP OPs Manager C: Controllers I: ANSP Manager	Procedure in Operations manuals
7.5.3 [Arg 4.2]	STCA status information continuously monitored and acted upon as required	Establish that formal process exists and is documented and applied	Written procedure Confirmation of use	No adverse reports	L: ANSP Operations D: ANSP ATC Supervisor C: Controllers I: ANSP Manager	Procedure in Operations manuals
7.5.4 [Arg 4.2]	STCA performance monitored and analysed to ensure that it does not degrade and continues to provide a substantive safety benefit	Establish that formal process exists and is documented and applied	Written procedure Confirmation of use	Percentage of conflicts eligible for STCA protection alerted to ATC remains consistently in line with expectations.	L: ANSP Operations D: ANSP Eng Manager C: STCA Technical Expert I: ANSP Manager	Procedure in Operations manuals

TABLE 7.5 STRATEGY FOR ASSURANCE –OPERATION & MAINTENANCE

END OF DOCUMENT