Consolidated baseline framework for Safety & Performance evaluation of STCA

Document information	
Project title	Evolution of ground-based safety nets
Project N°	04.08.01.
Project Manager	DSNA
Deliverable Name	Consolidated baseline framework for Safety & Performance evaluation of STCA
Deliverable ID	D03-SPR-STCA-V2
Edition	00.01.00

Please complete the advanced properties of the document

Abstract

A consolidated framework for safety assurance and performance evaluation of Short-Term Conflict Alert (STCA) systems is described. The framework is intended as a baseline for use in SESAR 4.8.1 'Evolution of ground-based safety nets'. Collision avoidance is described in terms of an operational service supported by ground based and airborne safety nets. SESAR Step 1 time based operations is assumed for describing the operational environment of STCA. EUROCONTROL Operational requirements for STCA are updated with TCAS interoperability requirements from the EUROCONTROL sponsored project PASS (Performance and safety Aspects of STCA, full Study). EUROCONTROL safety requirements for STCA are traced to corresponding operational requirements. Quantitative safety requirements are generic and will need instantiating for a particular airspace. A summary of the associated safety assessment is included to support the safety requirements. Common quantitative performance requirements are not considered mature enough at this stage. Excerpts from the PASS final project report and dissemination workshop are included as an example of applying a similar framework to a specific airspace model to derive quantitative safety and performance requirements, and as an indication of current maturity.

Authoring & Approval

Prepared By		
Name & company	Position / Title	Date
[redacted] EUROCONTROL	[redacted]	1st March 2011

Reviewed By		
Name & company	Position / Title	Date
[redacted] EUROCONTROL	[redacted]	21st January 2011
[redacted] /EUROCONTROL		7th February 2011
[redacted] EUROCONTROL		8th February 2011
[redacted] DSNA		10th February 2011
[redacted] DSNA		11th February 2011
[redacted] AENA		21st February 2011
[redacted] NATS		25th February 2011
[redacted] SELEX		25th February 2011

Approved By		
Name & company	Position / Title	Date
[redacted] DSNA	[redacted]	2nd March 2011
[redacted] EUROCONTROL		28th February 2011
[redacted] SELEX		25th February 2011
[redacted] NATS		2nd March 2011
[redacted] ENAV		2nd March 2011

Document History

Edition	Date	Status	Author	Justification
00.00.01	19th January 2011	Draft	EUROCONTROL	Initial draft distributed internally at EUROCONTROL
00.00.02	24th January 2011	Draft	EUROCONTROL	Updated after EUROCONTROL internal review
00.00.03	4th February 2011	Draft	EUROCONTROL	Updated after review meeting between EUROCONTROL and DSNA
00.00.04	11th February 2011	Draft	EUROCONTROL	Updated after review by EUROCONTROL and DSNA
00.01.00	1st March 2011	Final	EUROCONTROL	Updated after review comments from AENA, NATS, DSNA and SELEX

Intellectual Property Rights (foreground)

The foreground of this deliverable is owned by the SJU.

Table of Contents

List of tables

List of figures

Executive summary

A consolidated framework for safety assurance and performance evaluation of Short-Term Conflict Alert (STCA) systems is described. The framework is intended as a baseline for use in SESAR 4.8.1 'Evolution of ground-based safety nets'. Collision avoidance is described in terms of an operational service supported by ground based and airborne safety nets. SESAR Step 1 time based operations is assumed for describing the operational environment of STCA. EUROCONTROL Operational requirements for STCA are updated with TCAS interoperability requirements from the EUROCONTROL sponsored project PASS (Performance and safety Aspects of STCA, full Study). EUROCONTROL safety requirements for STCA are traced to corresponding operational requirements. Quantitative safety requirements are generic and will need instantiating for a particular airspace. A summary of the associated safety assessment is included to support the safety requirements. Common performance requirements are not considered mature enough at this stage. Excerpts from the PASS final project report and dissemination workshop are included as an example of applying a similar framework to a specific airspace model to derive quantitative safety and performance requirements:

- Report on PASS project dissemination workshop (summary of methods, tools and results) and debriefing with the SPIN (Safety nets Performance Improvement Network) sub-group held in November 2010.
- Examples of STCA safety and performance requirements for a particular airspace model.

An indication of the current status and maturity of this framework and its use is given by the following overall recommendations from the PASS workshop and EUROCONTROL SPIN sub-group debriefing report:

a) The PASS results should be further developed and validated in SESAR.
b) The SPIN Sub-Group should continue to support the safety nets development work in SESAR.
c) The following actions should be considered regarding SPIN Sub-Group support to refinement and validation of candidate operational, safety and performance requirements in SESAR:
    - Review the performance indicators that were used in the PASS project;
    - Determine how these performance indicators can be measured in a local context; and
    - Perform measurements in as many local environments as possible.
d) An agreed overall process should be established for incorporation of mature results of SESAR safety nets development work into existing EUROCONTROL specifications and guidance material.
e) Active awareness creation and promotion of best practices regarding safety nets should be continued.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to describe a baseline framework for safety and performance evaluation of Short Term Conflict Alert (STCA). The SESAR SPR (Safety and Performance Requirements) template is used to structure the framework.

1.2 Scope

SESAR Step 1 time based operational environment is assumed from 2013 and the intended European Operational Concept Validation Methodology (E-OCVM) maturity level is V2 'Feasibility'.

1.3 Intended audience

This document is intended for members of: 4.8.1 and 10.4.3 for use in evaluating safety and performance aspects of STCA. It may also be useful for members of 4.8.1, 4.8.2 and 4.8.3 involved in evaluation of safety and performance of other safety nets.

1.4 Structure of the document

- Chapter 1 introduces the need for deriving STCA safety and performance requirements and the current state of development in Europe.
- Chapter 2 summarises the collision avoidance operational concept in terms of services supported by safety nets and then describes the operational environment of STCA (Note: Detailed Operational Descriptions (DOD) and Operational Service and Environment Definition (OSED) were not available at the time of writing this draft.)
- Chapter 3 defines safety requirements with traces to corresponding operational requirements derived from a EUROCONTROL specification with updates from the Performance and safety Aspects of Short term conflict alert, full Study (PASS).
- Chapter 4 includes references and applicable documents.
- Appendix A contains EUROCONTROL operational requirements for STCA with updates proposed by PASS.
- Appendix B summarises the high level safety assessment used to derive the safety requirements.
- Appendix C reports on the PASS dissemination workshop and Safety nets Performance Improvement Network (SPIN) sub-group debriefing including recommendations for SESAR.
- Appendix D & E give examples of safety and performance requirements respectively from the PASS project based on a particular airspace model.

1.5 Background

Following the tragic mid-air collision over Überlingen, Germany on 1st July 2002 a number of strategic safety actions were initiated, amongst which were:

- Development of EUROCONTROL specifications and guidance material for ground-based safety nets, in particular STCA and
- Study of the feasibility of Airborne Collision Avoidance System (ACAS) Resolution Advisory (RA) downlink display at the Controller Working Position (CWP).

The EUROCONTROL SPIN (Safety Nets: Planning Implementation & eNhancements) Task Force was created in 2005 to draft standards and guidance material for the ground-based safety nets (STCA, Minimum Safe Altitude Warning (MSAW), and Area Proximity Warning (APW)).

In 2006 the EUROCONTROL STCA specification was finalised and a two-year period commenced during which European Air Navigation Service Providers (ANSPs) would make their STCA systems compliant with this specification in order to harmonise, in qualitative terms, the performance characteristics of these STCA systems. Further refinement, in quantitative terms, of the performance characteristics was believed to be necessary in order to improve the compatibility of ACAS and STCA. A feasibility evaluation was then performed to determine how the encounter model-based methodology used in ACAS safety studies could be used to study performance and safety aspects of STCA.

Also in 2006, a workshop was conducted to discuss research findings regarding RA downlink display at the CWP. The workshop concluded that such use of RA downlink would be technically feasible and operationally beneficial; however, the benefits could not be quantified due to lack of information about ACAS behaviour in European airspace.

Thus, the PASS (Performance and safety Aspects of Short-term conflict alert – full Study) project was initiated in order to develop:

- Elements for decision-making regarding RA downlink;
- Inputs for consistent overall concept for airborne and ground-based safety nets; and
- Recommendations for further standardisation of STCA.

In 2008, the SPIN task force became a sub-group under the changed name Safety nets Performance Improvement Network to develop and support the implementation and use of standards and guidance material for G-SNETs which also included Approach Path Monitor.

In November 2010, PASS held a final dissemination forum. A set of methods and tool specifications for evaluating safety and performance of STCA were presented. Quantitative safety and performance requirements were derived for an airspace model developed in PASS. At a subsequent SPIN debriefing recommendations were made. One of the main points made was that SPIN did not consider the quantitative safety and performance requirements developed by PASS to be mature enough to update the EUROCONTROL specifications and guidance material.

In November 2010 SESAR 4.8.1.4 started Task 4.2 to “Consolidate baseline framework for evaluation of safety and performance aspects of STCA (c.f. PASS phase 3). The task description is:

“To consolidate the safety assurance and performance evaluation framework for STCA developed in the EUROCONTROL PASS project. This framework will build upon the specifications and guidelines for optimisation developed by the SPIN-Sub-Group for a reference STCA system in Europe. Initial quantified safety and performance requirements will also be proposed in complement to the qualitative requirements contained in the SPIN material.”

This report is the deliverable output from the above task.

1.6 Acronyms and Terminology

Term	Definition
ACAS	Airborne Collision Avoidance System
Alert	Indication of an actual or potential hazardous situation that requires particular attention or action. (SPIN definition).
Altitude	The vertical distance of a level, a point or an object considered as a point, measured from mean sea level (MSL). (SPIN definition).
ANSP	Air Navigation Service Provider
APM	Approach Path Monitor
APW	Area Proximity Warning
ATC	Air Traffic Control

Term	Definition
ATM	Air Traffic Management
ATS	Air Traffic Service
ATS surveillance service	Term used to indicate a service provided directly by means of an ATS surveillance system. (SPIN definition).
CFL	Cleared Flight Level
Conflict	Conflict is any situation involving an aircraft and hazard in which the applicable separation minima may be compromised. Hazards are the objects or elements that an aircraft can be separated from. These are: other aircraft, terrain, weather, wake turbulence, incompatible airspace activity and, when the aircraft is on the ground, surface vehicles and other obstructions on the apron and manoeuvring area. Source: ICAO Doc. 9854 – Global Air Traffic Management Operational Concept Converging of aircraft in space and time which constitutes a predicted violation of a given set of separation minima. (SPIN definition).
DAPs	Downlinked Aircraft Parameters
E-OCVM	European – Operational Concept Validation Methodology
ECTL	EUROCONTROL Agency
EHS	Enhanced Surveillance (Mode S)
ELS	Elementary Surveillance (Mode S)
False alert	Alert which does not correspond to a situation requiring particular attention or action (e.g. caused by split tracks and radar reflections). (SPIN definition).
G-SNET	Ground-based Safety NET - A ground-based safety net is functionality within the ATM system that is assigned by the ANSP with the sole purpose of monitoring the environment of operations in order to provide timely alerts of an increased risk to flight safety which may include resolution advice. (SPIN definition).
Hazard	Any condition, event or circumstance that could induce an accident Source ICAO Doc. 9854 – Global Air Traffic Management Operational Concept
IAS	Indicated Airspeed
LOS	Loss Of Separation
MCP / FCU	Mode Control Panel (Boeing) / Flight Control Unit (Airbus)
Mid-air collision	Collision between aircraft both in airborne phase of flight
Missed Alert	A lack of indication to an actual or potential hazardous situation that requires particular attention or action.
Mode S	Secondary Surveillance Radar Mode Select
MSAW	Minimum Safe Altitude Warning System
Nuisance alert	Alert which is correctly generated according to the rule set but is considered operationally inappropriate. (SPIN definition).
PASS	Performance and safety Aspects of STCA, full Study

Term	Definition
Separation	Spacing between aircraft, levels or tracks. (SPIN definition).
SESAR	Single European Sky ATM Research Programme
SFL	Selected Flight Level (also referred to as Selected Altitude)
Short Term Conflict Alert	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. (SPIN definition).
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SNET	Safety Net
SPIN	EUROCONTROL Safety nets Performance Improvement Network
SPR	Safety and Performance Requirements
SSR	Secondary Surveillance Radar
STCA	Short-Term Conflict Alert
TAS	True Airspeed
TCAS	Traffic alert and Collision Avoidance System
VFR	Visual Flight Rules
Warning time	The amount of time between the first indication of an alert to the controller and the predicted hazardous situation. *Note – The achieved warning time depends on the geometry of the situation.* *Note – The maximum warning time may be constrained in order to keep the number of nuisance alerts below an acceptable threshold.* *(SPIN definition).*

2 Summary of Operational Concept

2.1 Description of the Concept Element

2.1.1 Collision avoidance

Collision avoidance is the third layer of conflict management and must activate when the separation mode has been compromised. Collision avoidance systems are not included in determining the calculated level of safety required for separation provision. Collision avoidance systems are, however, considered as part of ATM safety management. The collision avoidance functions and the applicable separation mode, although independent, must be compatible. Collision avoidance systems may be airborne or ground based.
Note: Separation provision and collision avoidance may overlap in time

2.1.2 Hazards

In the context of separation, ICAO defines hazards as "…objects or elements that an aircraft can be separated from. These are: other aircraft, terrain, weather, wake turbulence, incompatible airspace activity and, when the aircraft is on the ground, surface vehicles and other obstructions on the apron and manoeuvring area. For any hazard (i.e. any condition, event or circumstance that could induce an accident), a risk can be identified as the combination of the overall probability or frequency of occurrence of a harmful effect induced by the hazard, and the severity of that effect…"

2.2 Description of Operational Services

The collision avoidance operational service is supported by safety nets. Safety nets help prevent imminent or actual hazardous situations from developing into major incidents or even accidents. Safety nets, for airborne phases of flight and for preventing collision between aircraft and collision with terrain or obstacles, are either ground-based or airborne.

- Ground-based safety nets are an integral part of the ATM system. Using primarily ATS surveillance data, they provide warning times of up to two minutes. Upon receiving an alert, air traffic controllers are expected to immediately assess the situation and take appropriate action.
- Airborne safety nets provide alerts and resolution advisories directly to the pilots. Warning times are generally shorter, up to 40 seconds. Pilots are expected to immediately take appropriate avoiding action.

Ground based safety nets are intended to support a first layer of collision avoidance with airborne safety nets as the last resort

Note: Ground based safety nets and airborne safety nets may overlap in time.

2.2.1 Ground based safety nets

By the end of 2013 the following safety nets are expected to have been implemented throughout Europe:

- Short Term Conflict Alert (STCA)
- Minimum Safe Altitude Warning (MSAW)
- Area Proximity Warning (APW)
- Approach Path Monitor (APM)

2.2.1.1 Short Term Conflict Alert (STCA)

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 purpose of STCA is to detect and alert '**operationally relevant conflict**' involving at least one '**eligible aircraft**' with '**sufficient warning time**' for the controller to intervene and the aircraft to execute an appropriate manoeuvre.

This may be either to detect and alert on-time any of the following:

- predicted or actual infringement of separation minima for controlled flights (either IFR or VFR) to which ATC is expected to provide separation;
- hazardous encounters involving at least one controlled flight (either IFR or VFR) in situations where collision avoidance relies on visual separation by aircraft.

The sole purpose of STCA 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.

2.2.1.2 Minimum Safe Altitude Warning (MSAW)

MSAW is a ground-based safety net intended to warn the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of aircraft proximity to terrain or obstacles.

The sole purpose of MSAW is to enhance safety and its presence is ignored when calculating sector capacity.

MSAW is designed, configured and used to make a significant positive contribution to avoidance of controlled flight into terrain accidents.

2.2.1.3 Area Proximity Warning (APW)

APW is a ground-based safety net intended to warn the controller about unauthorised penetration of an airspace volume by generating, in a timely manner, an alert of a potential or actual infringement of the required spacing to that airspace volume.

This may be to detect and alert any of the following:

- uncontrolled (GA) aircraft infringing controlled airspace, or;
- commercial air traffic/controlled flight encroaching forbidden, restricted or danger areas;
- commercial air traffic/controlled flight exiting (excursions) from controlled airspace (or entering into a controlled airspace managed by another control unit).

The sole purpose of APW is to enhance safety and its presence is ignored when calculating sector capacity.

APW is designed, configured and used to make a significant positive contribution to prevention of accidents arising from unauthorised penetration of an airspace volume.

2.2.1.4 Approach Path Monitor

APM is a ground-based safety net intended to warn the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of aircraft proximity to terrain or obstacles during final approach.

The sole purpose of APM is to enhance safety and its presence is ignored when calculating sector capacity.

APM is designed, configured and used to make a significant positive contribution to avoidance of controlled flight into terrain accidents.

2.2.2 Airborne safety nets

Current airborne safety nets include:

- Airborne Collision Avoidance System (ACAS)
- Ground Proximity Warning System (GPWS)

2.2.2.1 Airborne Collision Avoidance System (ACAS)

The objective of ACAS is to provide advice to pilots for the purpose of avoiding potential collisions. This is achieved through resolution advisories (RAs), which recommend actions (including manoeuvres), and through traffic advisories (TAs), which are intended to prompt visual acquisition and to act as a precursor to RAs.

ACAS has been designed to provide a back-up collision avoidance service for the existing conventional air traffic control system while minimizing unwanted alarms in encounters for which the collision risk does not warrant escape manoeuvres. The operation of ACAS is not dependent upon any ground-based systems.

2.2.2.2 Ground Proximity Warning System (GPWS)

A ground proximity warning system (GPWS) is a system that provides automatically a timely and distinctive warning to the flight crew when the aeroplane is in potentially hazardous proximity to the earth's surface.

ICAO requires that a ground proximity warning system shall provide, as a minimum, warnings of the following circumstances:

a) excessive descent rate;

b) excessive terrain closure rate;

c) excessive altitude loss after take-off or go-around;

d) unsafe terrain clearance while not in landing configuration;

- •gear not locked down;
- •flaps not in a landing position; and

e) excessive descent below the instrument glide path.

2.3 Description of Operational Environment

2.3.1 SESAR Step 1 Time based operations

"Time Based Operations" is the building block for the implementation of the SESAR 2020 concept and is focused on flight efficiency, predictability and the environment. It follows on from SESAR Definition Phase IP1 service levels 0 and 1. "Time Based Operations" will encompass SESAR Definition Phase Service Level 2. The goal is a synchronised and predictable European ATM system, where partners are aware of the business and operational situations and collaborate to optimise the network. This first step initiates arrival airport time prioritisation together with wide use of data-link and the deployment of initial trajectory based operations through use of a controlled time of arrival to sequence traffic and manage queues. Traditional flight planning will be replaced by business trajectory and network operations planning enabled by system wide information management. The "airport" becomes an integral part of ATM and airspace users participate in ATM business decisions through user driven prioritisation processes. Required navigation performance will be used to systemise/optimise route structures, procedures and pilots, controllers and operations planners will have procedures, automation support and management tools bringing safety, environmental and flight efficiency improvements. Runway throughput is enhanced through new separation modes based on improved understanding of wake vortex dissipation and aircraft performance characteristics such as

brake to vacate. New modes of separation based on Airborne Separation Assistance System (ASAS) Spacing are envisaged in the TMA and 2D Precision Trajectory Clearance (PTC) en-route although these are not expected to modify the separation rules to be applied by ATC (and therefore the expected role of ground based safety-nets). Airport surface operations are optimised with planning and routing tools and the implementation of ATM related airport turn-round processes which will significantly improve planning and predictability. “Time Based Operations” projects build on mature concepts and technology that will be refined and validated through iterative prototyping using operational shadow mode and live trials as close to the target operational environment as possible. “Time Based Operations” development should be completed with ATM services and procedures together with system products delivered and ready for progressive initial operation capability with proven safety and performance benefits from 2013.

2.3.2 STCA

2.3.2.1 General

Figure 1 illustrates STCA and controller actions prompted by STCA (in grey boxes) interacting with other external components in a given operating environment (en-route or TMA). This figure is only depicting the STCA system in its nominal mode of operation. External components encompass pilot related actions after receiving an avoiding instruction. Note that technical aspects related to STCA, i.e. the components providing information to STCA to generate alerts such as the Surveillance Data Processing, Environment Data Processing and Flight Data Processing, have not been illustrated.

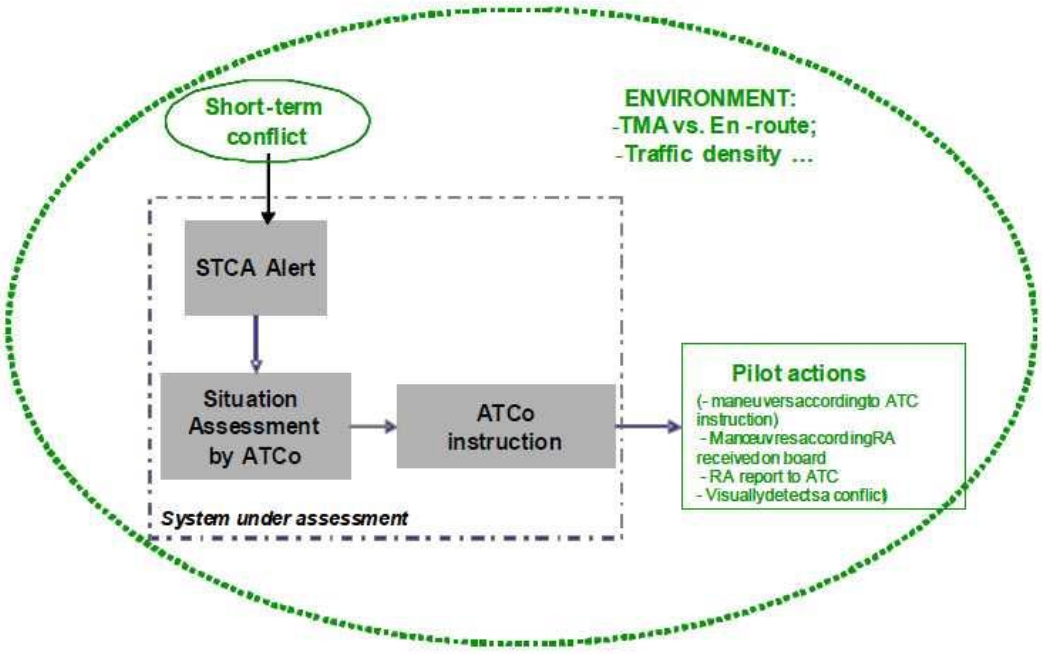

Figure 1 Boundaries of the STCA based safety net service (source PASS)

Figure 2 illustrates the nominal sequence of events to resolve a particular situation involving an STCA alert. It is a human centred system, with the Ground loop reflecting the states of the controller and the Air loop reflecting the corresponding states of the flight crew. For each state transition to occur certain preconditions have to be met and actions performed, complicated by many fixed or variable delays and anomalous cases.

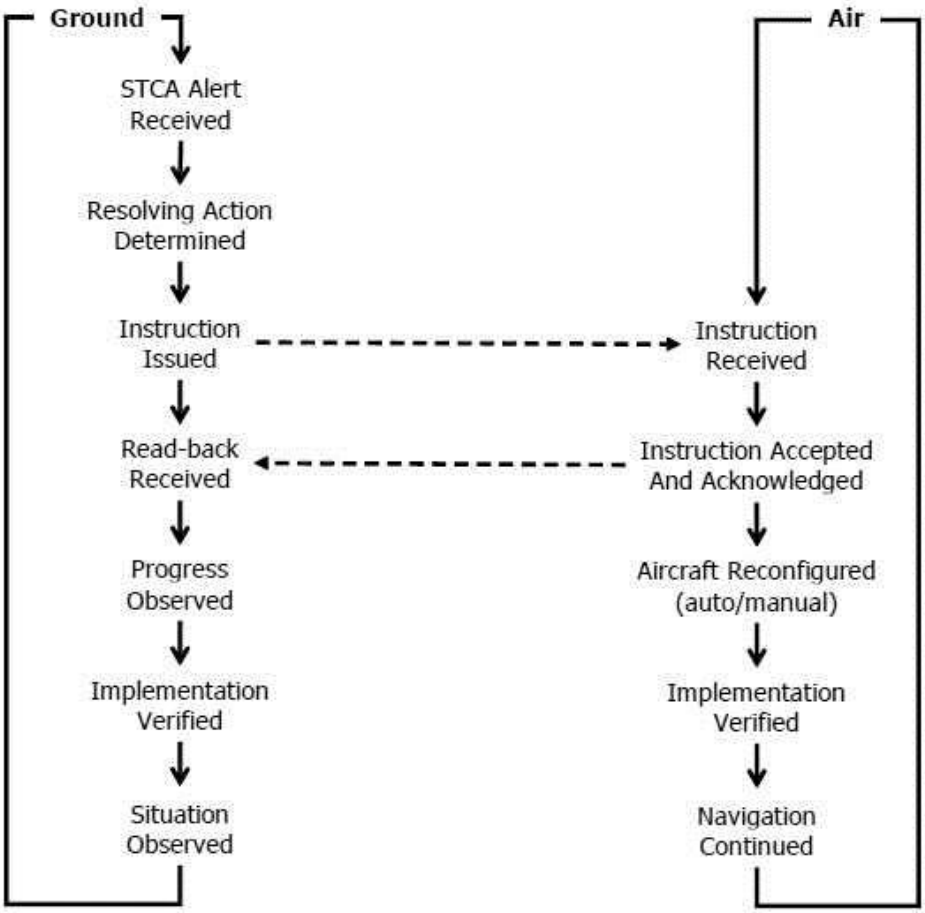

Figure 2 ATC control loop triggered by STCA (Source EUROCONTROL)

Although the sole goal of STCA is to prevent mid-air collisions (collision between aircraft both in airborne phase of flight), this goal may be achieved through different strategies which may overlap to varying degrees with the separation provision function and the airborne collision avoidance function. This is illustrated on the representation of conflict management in Figure 3.

Because the ground-based control loop is longer (and uses less frequent surveillance data) than the airborne control loop, the ATC collision prevention supported by STCA relies on the protection of “separation thresholds” (which may significantly differ from the applicable separation minima in order to limit the number of nuisance alerts during managed situations). These thresholds implicitly define a hazardous situation which the STCA shall help to prevent and which may differ from one local STCA implementation to another.

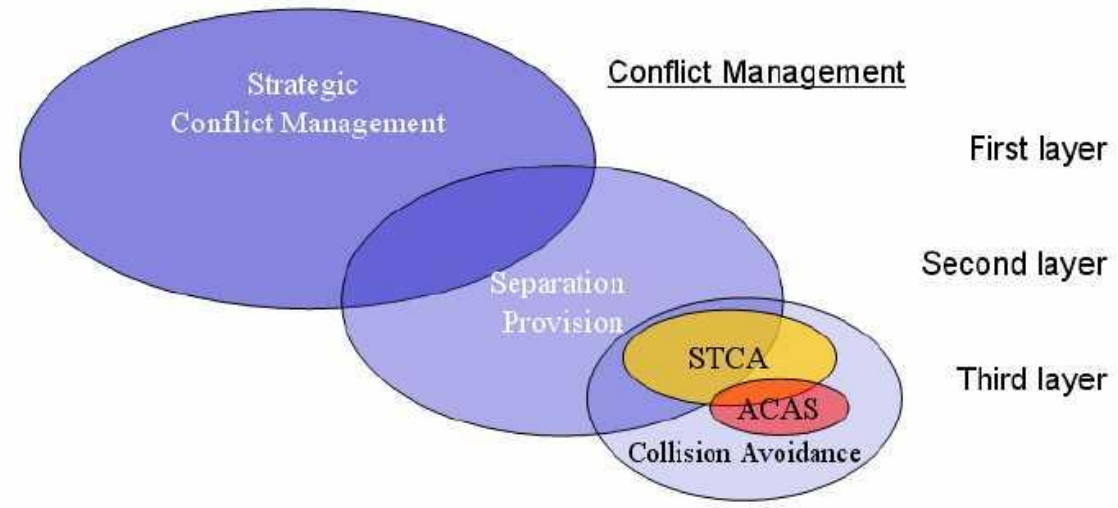

Figure 3 Position of STCA (and ACAS) within Conflict Management (Source PASS)

STCA is dependent on predicting loss of separation, and therefore particularly sensitive to:

- warning time (typically in range 80s to 120s)
- surveillance data
- traffic patterns
- separation standards

STCA should be capable of working in all controlled airspace with appropriate surveillance. Surveillance data quality should be sufficient to predict hazardous situations up to two minutes ahead.

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.

2.3.2.2 Airspace specific

Based on monitoring and modelling of European STCA environment (PASS) several approaches to the use of the STCA model have been identified and categorized. These categories first depend on the airspace in which STCA is operated. TMA airspace is characterized by lower applicable separation minima (3 NM and 1,000 ft) than in en-route airspace (5NM and 1,000 ft or 2,000 ft minima), which imposes different separation thresholds and warning time on STCA systems. Similarly, each ANSP's strategy may determine whether these STCA parameters are tuned towards more time-critical or less time-critical values and smaller or larger separation values.

2.3.2.2.1 En route

For en-route airspace, five families have been identified that correspond to increasingly tighter parameters for both the separation thresholds and the warning time used by the STCA in its trajectory prediction, and hence in its determination of alerts. These families and the different approaches to the use of STCA in en-route airspace are illustrated in Figure 4 below. LOS stands for Loss Of Separation.

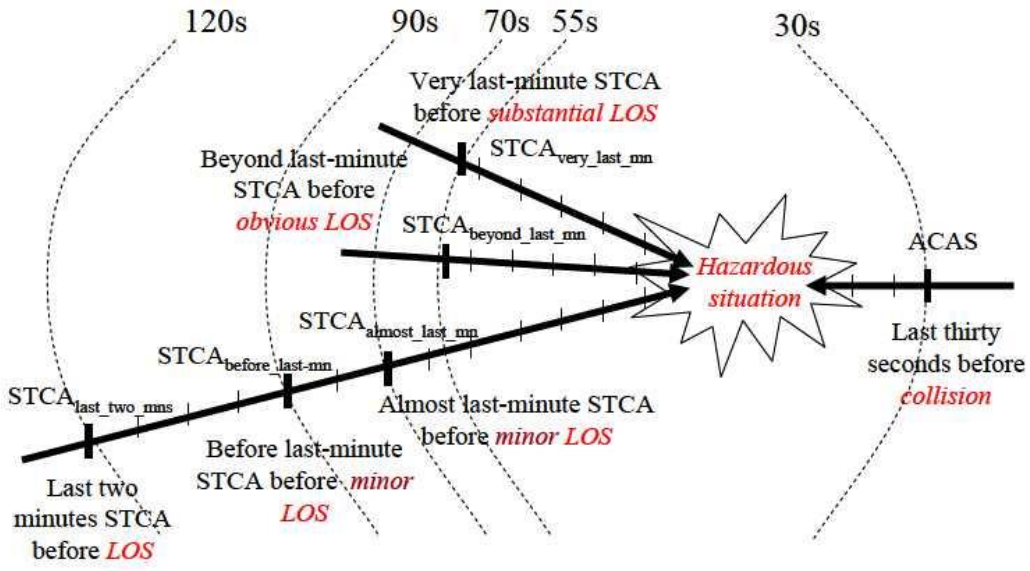

Figure 4 Families of STCA systems in en-route airspace (Source PASS)

2.3.2.2.2 TMA

For TMA, the identified families of STCA appear to use only two sets of parameters for separation thresholds, but each with two different warning times. These families and the different approaches to the use of STCA in TMA are illustrated in Figure 5.

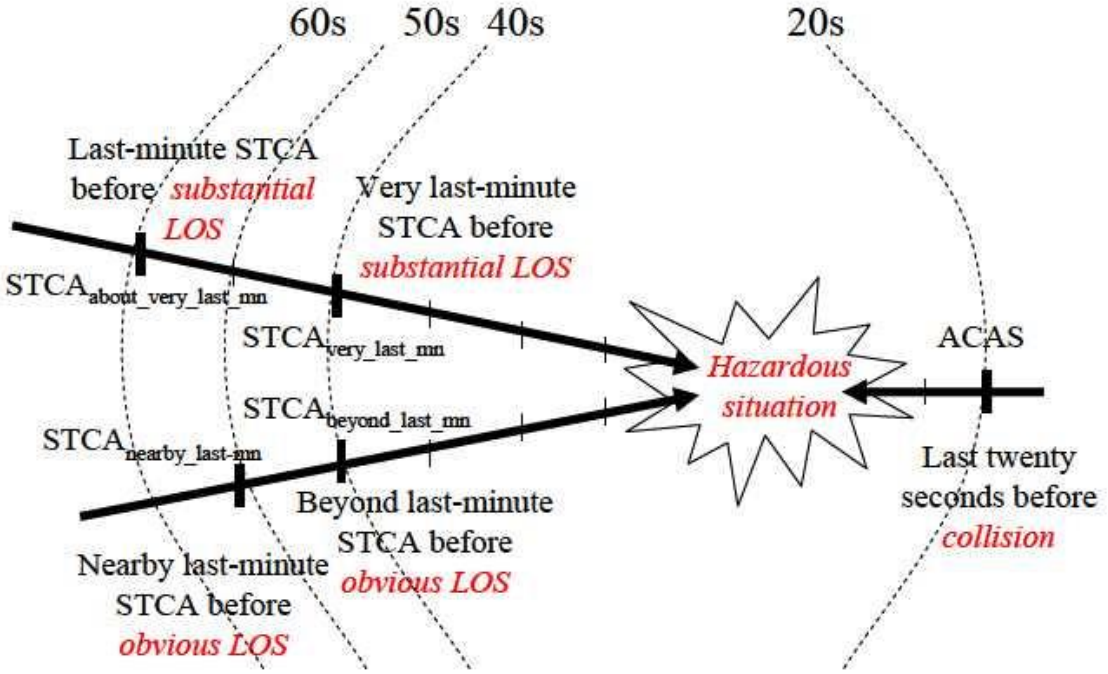

Figure 5 Families of STCA systems in TMA airspace (Source PASS)

3 Requirements

3.1 Ground based safety net

3.1.1 STCA

3.1.1.1 Safety Requirements

The following EUROCONTROL safety requirements [9] are intended to be common to all airspace. In the case of quantitative requirements a template is given intended to be instantiated with numerical values for specific real environments. Examples of quantitative safety requirements for a particular airspace model developed in the PASS project can be seen in Appendix D.

Each requirement has the following layout:

Identifier	
Requirement	

- *Identifier*: Requirement identification
- *Requirements*: Requirement text
- *Title*: Synthetic textual description of the object to be used for future reference.
- *Status*: Data life cycle (In Progress, Deleted)
- Importance: Data importance (Essential, Important, Desirable)
- *Rationale*: Requirement explanation if needed
- *Category*: Requirement category type (Operational, Service, System, Functional, Non Functional, Security, Safety, Performance, Interoperability)
- *V&V Method*: Requirement verification methods (Review of Design, Analysis, Inspection, Test)

Regarding the identifier, the following 4.8.1.project convention for the last 8 digits is proposed and followed:

Reference number 1 corresponds to the safety net i.e. 0010 is STCA, 0020 is MSAW, 0030 is APW and 0040 is APM.

Reference number 2 corresponds to the requirement number in default incremental units of ten where the last digit is reserved for numbering related requirements in a group,

e.g. REQ-04.08.01-SPR-0010.0030 is the third SPR requirement of STCA

or REQ-04.08.01-OSED-00100014 corresponds to the fourth OSED requirement in the first group (this is to handle mappings to external legacy IDs where letters have been used such as 1d).

To accommodate the SESAR Requirements (and V&V) Data Structures and Writing Guidelines [2], it is proposed that:

•Mandatory, recommended and optional requirements from the EUROCONTROL Specification are translated into “shall” requirements with different levels of importance.

•Initial requirements that use the operative verb “shall” are considered as “Essential” to claim compliance with the baseline operational service supported by STCA in all environments with ATS surveillance services.

•Initial requirements that use the operative verb “should” are considered as ”Important” to improve the operational, functional and performance aspects of STCA in all operational environments.

•Initial requirements that use the operative verb “may” are optional, but can be considered as ”Desirable” in some operational environments.

Identifier	REQ-04.08.01-SPR-0010.0010
Requirement	The probability of the STCA Processor failing shall not exceed To Be Determined (TBD)
	STCA processor reliability
	Hazard HA1 STCA alert warnings are not provided to the relevant controllers. Safety objective SO1 - The probability of total loss of STCA shall be no greater than TBD.

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0130	

Identifier	REQ-04.08.01-SPR-0010.0020
Requirement	The probability of the Radar Processor failing shall be not exceed TBD.
	Radar processor reliability
	Hazard HA1 STCA alert warnings are not provided to the relevant controllers. Safety objective SO1 - The probability of total loss of STCA shall be no greater than TBD.

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0130	

Identifier	REQ-04.08.01-SPR-0010.0030
Requirement	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)
	HMI reliability
	Hazard HA1 STCA alert warnings are not provided to the relevant controllers. Safety objective SO1 - The probability of total loss of STCA shall be no greater than TBD.

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0130	

Identifier	REQ-04.08.01-SPR-0010.0040
Requirement	All the data sets shall be validated for completeness and correctness in the relevant airspace and installed correctly.
	Validation of data sets
	Hazard HA2 STCA does not reliably capture and direct controller attention to potential conflicts. Safety Objective SO 2 - The probability of impaired functionality affecting the reliability of STCA shall be no greater than TBD

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0120, OSED-0010.0130	

Identifier	REQ-04.08.01-SPR-0010.0050
Requirement	The probability that the Alert inhibition process compromises the STCA function shall be TBD
	Alert inhibition reliability
	Hazard HA2 STCA does not reliably capture and direct controller attention to potentially conflicts. Safety Objective SO 2 - The probability of impaired functionality affecting the reliability of STCA shall be no greater than TBD

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0120, OSED-0010.0130	

Identifier	REQ-04.08.01-SPR-0010.0060
Requirement	The probability that STCA parameters are incorrect shall be TBD
	STCA parameter accuracy
	Hazard HA3 - The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be TBD Safety Objective SO 3 - The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be TBD

Identifier	REQ-04.08.01-SPR-0010.0070
Requirement	The probability that STCA performance is not monitored or analysed shall be shall be

	TBD
	STCA performance monitoring
	Hazard HA4 – The number of Nuisance Alerts and possible False Alerts (credible corruption) are above an acceptable level Safety Objective SO 4 - The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than TBD

		OSED-0010.0100, OSED-0010.0110	
Identifier	REQ-04.08.01-SPR-0010.0080		
Requirement	The probability that conflict prediction algorithms are not optimised or have become corrupted shall be TBD		
	Conflict prediction optimisation		
	Hazard HA4 – The number of Nuisance Alerts and possible False Alerts (credible corruption) are above an acceptable level Safety Objective SO 4 - The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than TBD		

		OSED-0010.0100, OSED-0010.0110	
Identifier	REQ-04.08.01-SPR-0010.0090		
Requirement	The probability that software configurations are inconsistent with air traffic procedures shall be TBD.		
	Software configuration consistency with air traffic procedures		
	Hazard HA4 – The number of Nuisance Alerts and possible False Alerts (credible corruption) are above an acceptable level Safety Objective SO 4 - The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than TBD		

		OSED-0010.0100, OSED-0010.0110	
Identifier	REQ-04.08.01-SPR-0010.0100		
Requirement	ATC procedures shall state what Controllers should do in the event of loss of an automatic alerting facility such as STCA.		
	ATC procedures for loss of automatic STCA alerting		
	Hazard HA1 – STCA alert warnings are not provided to the relevant controllers. Safety objective SO1 - The probability of total loss of STCA shall be no greater than TBD.		

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0130	
Identifier	REQ-04.08.01-SPR-0010.0110		
Requirement	Procedures shall be put in place to ensure that the Controller is advised of any system changes which might degrade the performance of STCA		
	Procedures for system degradation of STCA performance		
	Hazard HA2 STCA does not reliably capture and direct controller attention to potentially conflicts. Safety Objective SO 2 - The probability of impaired functionality affecting the reliability of STCA shall be no greater than TBD		

		OSED-0010.0070, OSED-0010.0080, OSED-0010.0090, OSED-0010.0130	
Identifier	REQ-04.08.01-SPR-0010.0120		
Requirement	The action to be taken when the number of nuisance Alerts is above acceptable limits shall be addressed in local instructions/regulations		
	Nuisance alerts above limits		
	Hazard HA4 – The number of Nuisance Alerts and possible False Alerts (credible corruption) are above an acceptable level. Safety Objective SO 4 - The probability of the number of nuisance alerts and false alerts exceeding acceptable levels shall be no greater than TBD		

		OSED-0010.0100, OSED-0010.0110	
Identifier	REQ-04.08.01-SPR-0010.0130		
Requirement	Controllers shall be adequately trained and competent so that the safety benefits of STCA can be realised operationally		
	Controller training		

	Hazard HA3 – - The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be TBD Safety Objective SO 3 - The probability that the Controller does not react effectively to resolve a conflict detected by STCA shall be TBD

3.1.1.2 Performance Requirements

Quantitative requirements are not mature enough to enter in this section at the moment. See Appendix C for status of consolidation process and Appendix E for examples of quantitative performance requirements proposed by PASS.

4 References and Applicable Documents

4.1 Applicable Documents

This SPR complies with the requirements set out in the following documents:

[1] IS SESAR SEMP 2.0

[2] IS SESAR Template Toolbox Latest version

[3] IS SESAR Requirements and V&V Guidelines Latest version

[4] IS SESAR Template Toolbox Users Manual Latest version

4.2 Reference Documents

The following documents were used to provide input/guidance/further information/other:

[5] Guidelines for approval of the provision and use of air traffic services supported by data communications, EUROCAE/RTCA, ED78A, 2000

[6] SESAR 4.8.1 “Evolution of ground-based safety nets”, Project Initiation Report, 15th September 2010

[7] Specification for Short Term Conflict Alert, EUROCONTROL, 19th May 2009

[8] Guidance material for Short Term Conflict Alert Appendix A: Reference STCA system, EUROCONTROL, 19th May 2009

[9] Guidance material for Short Term Conflict Alert Appendix B-3: Outline Safety Case for STCA system, EUROCONTROL, 19th May 2009

[10] PASS Final report – Synthesis and guidelines, EUROCONTROL, 12th November 2010

[11] European – Operational Concept Validation Methodology, Version 3, EUROCONTROL, February 2010

[12] EUROCONTROL Safety Regulatory Requirement (ESARR) 4 – Risk Assessment and Mitigation in Air Traffic Management, edition 1.0, 5th April 2001

[13] EUROCONTROL Standard Document for Radar Surveillance in En-route Airspace and Major Terminal Areas (SUR.ET1.ST01.1000-STD-01-01, Edition 1.0 of March 1997)

[14] Global Air Traffic Management Operational Concept, ICAO, 2005.

[15] Procedures for Air Navigation Services Air Traffic Management, ICAO, Doc 4444 ATM/501, 2007

[16] EUROCONTROL Safety Regulatory Requirement (ESARR) Explanatory Material on Ground Based Safety Nets, Edition 1.0, 15th April 2010

Appendix A Operational Requirements

A.1 General

The following requirements are derived from [7] and [10]

A.2 Policy, Organisational Clarity and Training Requirements

A.2.1 Policy

This section summarises the organisational requirements that call for a policy on the use of STCA at the ANSP level. These baseline operational requirements are derived from the mandatory, recommended or optional requirements ("shall", "should" or "may") contained in the EUROCONTROL Specification for STCA [7].

Identifier	REQ-04.08.01-OSED-O010.0011
Requirement	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.

Identifier	REQ-04.08.01-OSED-0010.0012
Requirement	The policy on the use of STCA shall be consistent with the following generic policy statements, inter alia: a) STCA is a safety net; its sole purpose is to enhance safety and its presence is ignored when calculating sector capacity; and b) STCA is designed, configured and used to make a significant positive contribution to the effectiveness of separation provision and collision avoidance.

Identifier	REQ-04.08.01-OSED-0010.0013
Requirement	The policy on the use of STCA shall contain more detail or additional aspects called for by local factors.

Identifier	REQ-04.08.01-OSED-00100014
Requirement	The policy shall be communicated to all relevant staff in order to ensure consistency of all design, configuration, operational use and monitoring activities in compliance with the intended use of STCA.

A.2.2 Responsibility for Management of STCA

This section summarises the organisational requirements on the responsibility for management of STCA at the ANSP level. These baseline operational requirements are derived from the mandatory and recommended requirements ("shall" or "should") contained in the EUROCONTROL Specification for STCA [7].

Identifier	REQ-04.08.01-OSED-0010.0021
Requirement	The ANSP shall assign to one or more staff, as appropriate, the responsibility for overall management of STCA.

Identifier	REQ-04.08.01-OSED-0010.0022
Requirement	It shall be possible for other staff in the organisation to identify the assigned staff responsible for overall management of STCA.

Identifier	REQ-04.08.01-OSED-0010.0023
Requirement	The assigned staff responsible for overall management of STCA shall seek advice from the STCA manufacturer, as appropriate.

A.2.3 Training and Competence

This section summarises the organisational requirement ("shall") about training and competence on STCA at the ANSP level. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA [7].

Identifier	REQ-04.08.01-OSED-0010.0030
Requirement	The ANSP shall ensure that all controllers concerned are given specific STCA training and are assessed as competent for the use of the relevant STCA system. Note.– 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).

A.3 Requirements on Procedures

A.3.1 Local instructions

This section summarises the procedural requirement that calls for local instructions for the use of STCA at the ANSP level. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA [7] and complies with existing ICAO PANS-ATM provisions for STCA (cf. Doc 4444, section 15.7.2 "Short-term conflict alert (STCA) procedures").

Identifier	REQ-04.08.01-OSED-0010.0040
Requirement	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.

A.3.2 Controller Actions

This section summarises the procedural requirement that applies to controller in the event of an STCA alert. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA[7].

It complements existing ICAO PANS-ATM provisions for STCA (cf. Doc 4444, section 15.7.2 "Short-term conflict alert (STCA) procedures") as it also addresses the specific circumstances of an alert being generated while the separation minima are already infringed.

Identifier	REQ-04.08.01-OSED-0010.0050
Requirement	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. Note.– STCA does not exist in isolation; when a pilot reports a manoeuvre induced by a TCAS resolution advisory (RA), the controller is required not to attempt to modify the aircraft flight path.

Performance analyses

This section summarises the procedural requirement that calls for regular STCA performance analyses at the ANSP level. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA. [7].It supplements existing ICAO PANS-ATM provisions for STCA (cf. Doc 4444, section 15.7.2 “Short-term conflict alert (STCA) procedures”), which only call for statistical analyses of justified alerts.

Identifier	REQ-04.08.01-OSED-0010.0061
Requirement	STCA performance shall be analysed regularly to identify possible shortcomings related to STCA.

A.3.4 Statistical Analyses

This section summarises the organisational and procedural requirements that relate to STCA statistical analyses. These baseline operational requirements are derived from the recommended requirements (“should”) contained in the EUROCONTROL Specification for STCA [7], which comply with existing ICAO PANS-ATM provisions for STCA (cf. Doc 4444, section 15.7.2 “Short-term conflict alert (STCA) procedures”).

Identifier	REQ-04.08.01-OSED-0010.0062
Requirement	The appropriate ATS authority shall retain electronic records of all STCA alerts generated.

Identifier	REQ-04.08.01-OSED-0010.0063
Requirement	The data and circumstances pertaining to each STCA alert shall be analysed to determine whether an alert was justified or not.

Identifier	REQ-04.08.01-OSED-0010.0064
Requirement	Non-justified STCA alerts, e.g. when visual separation was applied, shall be ignored.

Identifier	REQ-04.08.01-OSED-0010.0065
Requirement	A statistical analysis shall be made of justified STCA alerts in order to identify possible shortcomings in airspace design and ATC procedures as well as to monitor overall safety levels.

A.4 Requirements on STCA Capabilities

A.4.1 Alerting performance

This section summarises the functional and performance requirements that apply to STCA alerting performance. These baseline operational requirements are derived from the mandatory or optional requirements (“shall” or “may”) contained in the EUROCONTROL Specification for STCA[7].

Identifier	REQ-04.08.01-OSED-0010.0070
Requirement	STCA shall detect operationally relevant conflicts involving at least one eligible aircraft.

Identifier	REQ-04.08.01-OSED-0010.0080
Requirement	STCA shall alert operationally relevant conflicts involving at least one eligible aircraft. Note.– Conflicts are operationally relevant when covered by the adopted rule set and optimisation strategy. The rule set and optimisation strategy should be determined taking into account the relevant local factors. STCA should not be expected to alert all operationally relevant conflicts.

Identifier	REQ-04.08.01-OSED-0010.0091
Requirement	STCA alerts shall attract the controller's attention.

Identifier	REQ-04.08.01-OSED-0010.0092
Requirement	STCA alerts shall identify the aircraft involved in the conflict.

Identifier	REQ-04.08.01-OSED-0010.0093
Requirement	STCA alerts shall be at least visual.

Identifier	REQ-04.08.01-OSED-0010.0094
Requirement	An audible element shall be included to improve the STCA systems ability to draw the controller's attention to the alert where necessary. Note.– Human factors and local circumstances determine whether or nor audible alerts are necessary.

Identifier	REQ-04.08.01-OSED-0010.0095
Requirement	If a continuous audible element is included in STCA, an acknowledgement mechanism shall be provided to silence an alert.

Identifier	REQ-04.08.01-OSED-0010.0100
Requirement	The number of nuisance alerts produced by STCA shall be kept to an effective minimum. Note.– Human factors and local circumstances determine what constitutes an effective minimum.

Identifier	REQ-04.08.01-OSED-0010.0110
Requirement	The number of false alerts produced by STCA shall be kept to an effective minimum. Note.– Local circumstances determine what constitutes an effective minimum.

A.4.2 Warning time

This section summarises the functional and performance requirements that apply to STCA warning time. These baseline operational requirements are extracted from the EUROCONTROL Specification for STCA[7].

Identifier	REQ-04.08.01-OSED-0010.0120
Requirement	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. Note.– Insufficient warning time may be provided in cases of sudden, unexpected manoeuvres.

Identifier	REQ-04.08.01-OSED-0010.0130
Requirement	STCA shall continue to provide alert(s) as long as the alert conditions exist.

Alert inhibition

This section summarises the functional requirements that deal with STCA alert inhibition. These baseline operational requirements are derived from the mandatory requirements (“shall”) contained in the EUROCONTROL Specification for STCA [7].

Identifier	REQ-04.08.01-OSED-0010.0141
Requirement	STCA shall provide the possibility to inhibit alerts for predefined volumes of airspace to suppress unnecessary alerts.

Identifier	REQ-04.08.01-OSED-0010.0142
Requirement	STCA shall provide the possibility to inhibit alerts for individual flights to suppress unnecessary alerts.

Identifier	REQ-04.08.01-OSED-0010.0150
Requirement	Alert inhibitions shall be made known to all controllers concerned.

A.4.4 Status information

This section summarises the functional requirement that calls for the provision of STCA status information on CWP. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA [7]

Identifier	REQ-04.08.01-OSED-0010.0160
Requirement	Status information shall be presented to supervisor and controller working positions in case STCA is not available.

A.4.5 Data recording

This section summarises the functional requirement that calls for the availability of STCA data recordings. This baseline operational requirement is extracted from the EUROCONTROL Specification for STCA [7]

Identifier	REQ-04.08.01-OSED-0010.0170
Requirement	All pertinent STCA data shall be made available for off-line analysis. Note.– Off-line analysis may need access to other data sources as well (surveillance data and voice recordings) for complete analysis.

A.4.6 Adaptability

This section summarises the functional requirements that call for STCA adaptability to airspace and traffic characteristics at any time and under different conditions (e.g. in RVSM airspace, in case of system degradation, etc). These baseline operational requirements are derived from the recommended or optional requirements ("should" or "may") contained in the EUROCONTROL Specification for STCA [7].

Identifier	REQ-04.08.01-OSED-0010.0181
Requirement	STCA shall be adaptable for the procedures in use in all distinct volumes of airspace at any moment in time.

Identifier	REQ-04.08.01-OSED-0010.0182
Requirement	STCA shall take into account the specific volume of airspace in which each aircraft is flying, in order to apply appropriate parameters or trajectory estimation.

Identifier	REQ-04.08.01-OSED-0010.0183
Requirement	Different parameters shall be applied in the case of system degradation (e.g. unavailability of one or more radar stations).

Identifier	REQ-04.08.01-OSED-0010.0184
Requirement	In RVSM airspace, STCA shall 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.

A.4.7 Interoperability with TCAS

The following requirements are derived from PASS [10]

Identifier	REQ-04.08.01-OSED-0010.0191
Requirement	When a time-critical avoiding instruction is deemed necessary in reaction to an STCA alert, the controller shall use avoiding action phraseology to prompt pilot quick response. Note: a prompt pilot response normally has the positive side-effect of preventing the occurrence of TCAS resolution advisories.
Identifier	REQ-04.08.01-OSED-0010.0192
Requirement	When an avoiding instruction is deemed necessary in reaction to an alert, the controller shall use horizontal instructions each time it is permitted by the current situation to ensure maximum compatibility with potential TCAS resolution advisories. Note: elements of the current situation to consider include encounter geometry, quality of radar detection and lack of ambiguity in the radar identification. Note: horizontal avoiding instructions with significant heading alteration are likely to prompt quick pilot response and shorten the period of aircraft convergence, thus increasing the likelihood of preventing the occurrence of TCAS resolution advisories.

	The model-based performance evaluation (WA2) demonstrated that, for an STCA primarily designed to 'make a significant positive contribution to the effectiveness of collision prevention essentially', "avoiding instructions should be preferably given in the vertical dimension so as to reduce the likelihood of a subsequent TCAS RA (since horizontal instructions are less effective in increasing safety margins, and hence to prevent RA issuance). However, belated vertical avoiding instructions have a greater potential for being contrary to a subsequent RA if and when it happens." ([D170]) This trend was also highlighted in the monitoring activity (WA1) during the consolidated analysis of a set of events of interest [W42] which showed that • "Horizontal actions were effective (i.e. increased significantly the miss distance, for example from 1 to 2 Nm, for a minimum separation of 3Nm) in 3 cases among the 10 retained: events 8, 9, 11 on one aircraft in all 3 cases." • "[…] Vertical instructions were ineffective in 3 cases: events 3, 6 and 8 (on one aircraft). [...] In event 6 the ATC instruction was ineffective because it was opposite to the TCAS RA received just when the pilot was initiating the ATC instruction. The pilot followed this RA.

Identifier	REQ-04.08.01-OSED-0010.0193
Requirement	STCA alerts shall also attract the attention of controllers from adjacent sectors to allow them to warn the controller in which sector the alert is occurring.

Identifier	REQ-04.08.01-OSED-0010.0194
Requirement	STCA shall take into account information on actual or possible future aircraft trajectory to reduce the number of nuisance alerts during aircraft manoeuvres complying with standard ATC procedures.

Identifier	REQ-04.08.01-OSED-0010.0195
Requirement	When the geometry of the situation permits having sufficient warning time, the number of short duration alerts shall be kept to an effective minimum.

Identifier	REQ-04.08.01-OSED-0010.0196
Requirement	The number of split alerts shall be kept to an effective minimum.

Appendix B Assessment / Justifications

B.1Safety and Performance Assessments

B.1.1 Safety assessment

The following summary is based on EUROCONTROL Guidance Material for Short term Conflict Alert Appendix B-3 Outline Safety case for STCA System. [9]

B.1.1.1 Summary of the Operational Hazard Assessment

The functions specified in the EUROCONTROL Specification for STCA were subjected to EUROCONTROL Safety Assessment Method 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.

The FHA results are set out in Table 1. 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 D10 on how to do this. Safety Objectives have been expressed in terms of probability although no values have been assigned (left as To Be Determined (TBD)) in Table 1 as this is a matter for ANSPs to address and mitigation measures have been identified for each hazard.

The Safety Objectives are derived from the FHA and are summarised in the Table 2 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.

Figure 6 shows the fault tree used to derive the safety requirements given in Section 3

Table 1 STCA functional hazard analysis

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)*

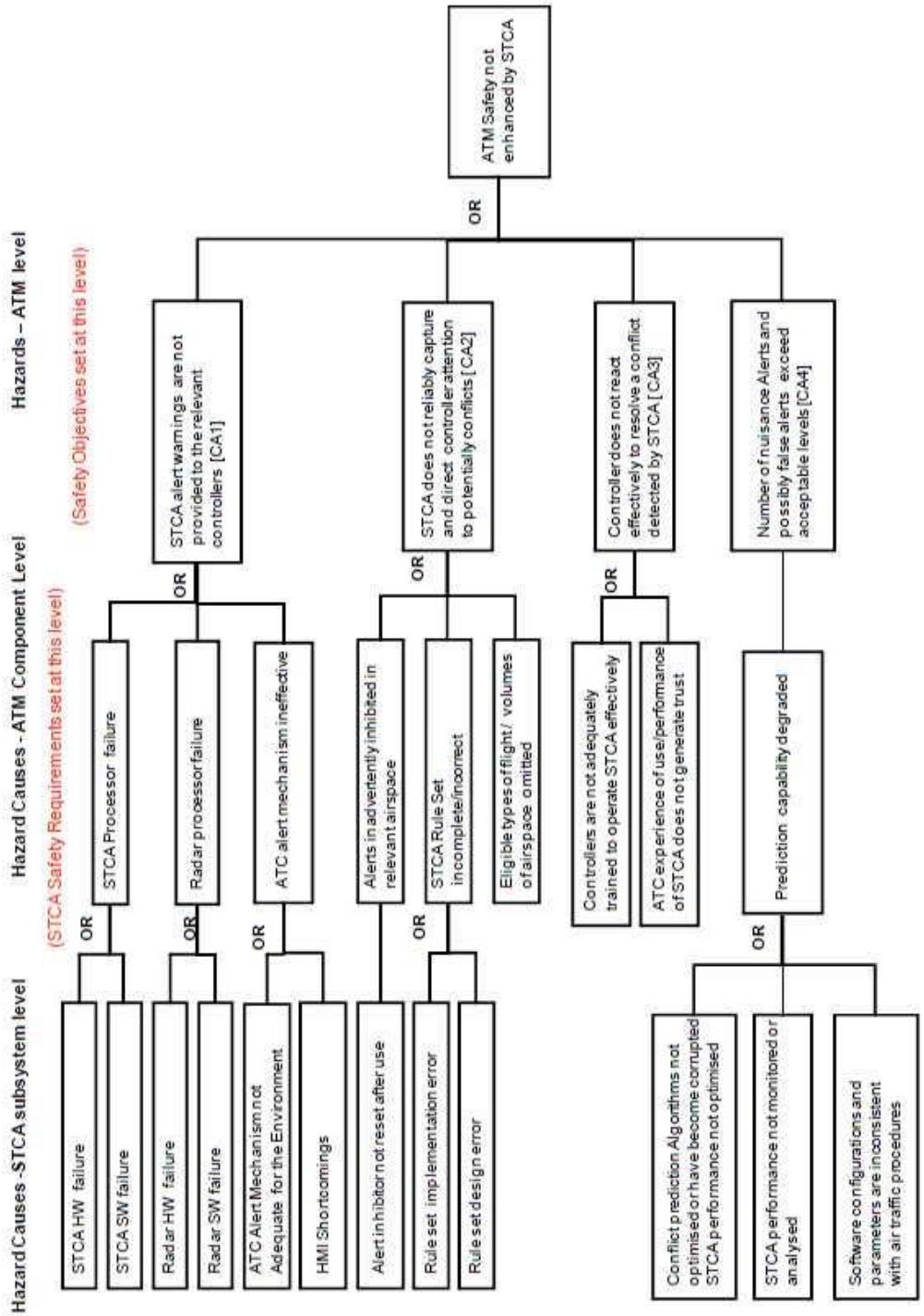

Figure 6 Fault tree for ATM safety not enhanced by STCA

Table 2 Safety objectives

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*

Appendix C PASS dissemination workshop & SPIN group debriefing report

C.1 Introduction

The full title of this report is PASS (Performance and safety Aspects of Short term conflict alert, full Study) Dissemination Workshop and SPIN (Safety nets Performance Improvement Network) Sub-Group Debriefing Report.

C.1.1 Background and context

Following the tragic mid-air collision over Überlingen, Germany on 1st July 2002 a number of strategic safety actions were initiated, amongst which were:

- Development of EUROCONTROL specifications and guidance material for ground-based safety nets, in particular Short Term Conflict Alert (STCA); and
- Study of the feasibility of Airborne Collision Avoidance System (ACAS) Resolution Advisory (RA) downlink display at the Controller Working Position (CWP).

In 2006 the EUROCONTROL STCA specification was finalised and a two-year period commenced during which European Air Navigation Service Providers (ANSPs) would make their STCA systems compliant with this specification in order to harmonise, in qualitative terms, the performance characteristics of these STCA systems. Further refinement, in quantitative terms, of the performance characteristics was believed to be necessary in order to improve the compatibility of ACAS and STCA. A feasibility evaluation was then performed to determine how the encounter model-based methodology used in ACAS safety studies could be used to study performance and safety aspects of STCA.

Also in 2006, a workshop was conducted to discuss research findings regarding RA downlink display at the CWP. The workshop concluded that such use of RA downlink would be technically feasible and operationally beneficial; however, the benefits could not be quantified due to lack of information about ACAS behaviour in European airspace.

Thus, the PASS project was initiated in order to develop:

- Elements for decision-making regarding RA downlink;
- Inputs for consistent overall concept for airborne and ground-based safety nets; and
- Recommendations for further standardisation of STCA.

C.1.2 Scope and objectives of the PASS project

The scope of the PASS project was performance and safety aspects of STCA operations including technical, procedural & human performance aspects and considerations of the interactions with ACAS.

The objectives of the PASS project were:

- Progress towards standards for ground-based safety nets through quantified requirements for STCA by proposing candidate operational, safety and performance requirements; and
- Progress with an overall concept of operation for ground-based and airborne safety nets, ensuring compatible STCA and TCAS operations.

C.2 PASS Phase 1: Monitoring activity

The purpose of phase 1 of the PASS project was operational monitoring to develop a better understanding of STCA and ACAS operations, i.e. the typical sequence of events in ATM occurrences in which STCA and/or TCAS played a role and the factors that have a major influence on this sequence.

C.2.1 Operational monitoring scope, objectives and main achievements

The scope and objectives of phase 1 of the PASS project were:

- Develop a better understanding of the typical sequence of STCA/TCAS related events, through statistical analysis of STCA and TCAS occurrences;
- Determination of environmental, technical and human influencing factors, through specific analysis (by operational experts) of a subset of occurrences of interest; and
- Evaluations of RA downlink reliability and development of an operational view of ACAS performance that RA downlink can provide, through specific analysis of recorded TCAS occurrences.

In total 180 occurrences were selected for statistical analyses. This was considered sufficient to obtain statistically relevant results. But the amount of effort available for this phase, being about three man-years, did not allow detailed examination of sufficient occurrences to allow exhaustive determination of all influencing factors but nevertheless provided key inputs for phase 2 of the PASS project. (The points in this paragraph were emphasised during audience questioning.)

The results of the specific analysis of recorded TCAS occurrences were used as a major input for the second RA downlink workshop in October 2009.

C.2.2 Operational analysis of reported STCA and ACAS occurrences

The operational analysis of reported STCA and ACAS occurrences provided insight into the adequacy of STCA alerts in a range of different STCA systems. A significant proportion of alerts were observed to occur after separation minima had already been violated. This unexpected observation is due to parameter settings and encounter geometry. Nevertheless, in most cases STCA provides sufficient warning time allowing ATC to take corrective action.

Also TCAS RAs in most cases provide sufficient warning time allowing the pilot to ensure safe vertical separation at closest approach. The rate of non-response to RAs was found to be in the order of 10% to 20%. The pilots' TCAS RA report to ATC was often late or missing.

In about 70% of the occurrences of STCA alerts the air traffic controller (ATCO) issued avoiding instructions within 10 seconds after the alert, often in combination with traffic information. However, these numbers are not typical for STCA occurrences because the studied occurrences are biased towards the more serious cases.

Pilot manoeuvres were on average observed 15 seconds after ATC instructions. This correlates well with the the assertion made by the FAA that an alert with a duration of less than 22 seconds is a nuisance alert.

C.2.3 Analysis of recorded ACAS occurrences

A total of 880 ACAS occurrences were found in recordings from six Mode S radars in the European core area, covering about 1,330,000 flight hours. About 350,000 RA downlink messages were in the recordings, the vast majority being empty messages from a small number of aircraft.

Empty messages appear to be a European phenomenon, not observed in other parts of the world. For RA downlink display at the CWP this is not a major issue because they never correspond with a real RA annunciation in the cockpit and can easily be filtered out. (Detailed points about empty messages discussed during audience questioning.)

C.3 PASS Phase 2: Model-based operational performance assessment

The purpose of phase 2 of the PASS project was to address safety benefits of STCA through use of the encounter model-based methodology and to address safety assurance aspects of joint STCA and ACAS operations.

C.3.1 Setting-up the model-based performance evaluation framework

The model based performance framework consists of a set of models to simulate operationally realistic scenarios of a safety net environment and its use. The set includes models of: encounters, safety nets, pilot and ATCO, surveillance, and aircraft behaviour.

The distribution of modelled encounters is based on radar data from a variety of air ANSPs: NATS (UK), LVNL (Netherlands), DSNA (France), skyguide (Switzerland) and RLP (Czech Republic). Collected from October 2007 to March 2008, the data corresponds to about 3.4 million flight hours. (The use of real data was emphasised during replies to audience questioning.)

The surveillance model can be configured for TMA and en-route with Mode C, Mode S (100 feet and 25 feet) for a number of radars at different locations. There is a multi-radar tracking model with horizontal and vertical components.

The STCA model is based on the EUROCONTROL specification and can be tuned according to different airspaces. The ACAS model is based on the TCAS standard. ATCO model responses to STCA are emulated in a simple, yet realistic, manner based on actual air traffic controller responses observed during the monitoring phase (point emphasised during audience questioning). Pilot model responses to ATCOs are based on analysis of real pilot responses during monitoring of real operations. Significant model parameters are probability, timing and strength of a manoeuvre.

The ACAS pilot response model is based on analysis of airborne recordings of real events. There is a range of 32 discrete responses with varying initial delay, acceleration and vertical speeds.

C.3.2 Model-based evaluation and sensitivity analyses of STCA performances

Basic scenarios, a range of STCA configurations, and sensitivity analysis scenarios were inputs for the STCA simulations. Five STCA families (configuration type) were identified in en-route airspace and four in the TMA based on results of monitoring real systems. As part of the sensitivity analysis, pilot and ATCO behaviours were varied according to observations during the monitoring activity. Conflicts were classified according to initial and final encounter geometry severity. Collisions were not modelled because accidents were not observed during the monitoring phase (point made in response to audience questioning).

The likelihood of STCA alerts was measured by number of alerts per flight hour, per altitude band, per conflict severity etc. The relevance of alerts was measured i.e. proportion of nuisance or missed alerts. Metrics for efficacy of genuine STCA alerts were warning time left for the air traffic controller and achievable minimum separation. The compatibility of STCA with TCAS was measured by the number of conflicts with both STCA alert and TCAS RA.

C.3.3 Derivation of candidate performance requirements

Model based performance analysis of European STCA families, highlighted three main ANSP strategies for STCA implementation and optimisation: conservative, intermediate and liberal providing correspondingly extensive, substantial and limited separation protection respectively.

Quantified functional requirements are proposed for the alerting capability of STCA depending on ANSP strategy i.e. conservative, intermediate or liberal. Quantified performance requirements are derived e.g. for acceptable maximum proportion of nuisance alerts and acceptable maximum ratio of

short warning time alerts. These requirements are based on a generic model which would need to be further consolidated and developed up to pre-operational stage before operational use.

During audience questioning it was noted that there may be several strategies within a single STCA because of for example the differences in the way vertical and lateral may be handled, or regional differences in airspace.

C.3.4 Operational safety assessment of STCA and ACAS operations

C.3.4.1 Background and Context

According to the European Safety Regulation Commission (policy SRC28.6), ground based safety nets are confirmed to be part of the Air Traffic Management (ATM) system and, as such, subject to hazard identification as required by ESSAR 4 (EUROCONTROL Safety Regulatory Requirement risk assessment and mitigation in ATM). Risk assessment is to include potential negative effects of the interaction between STCA and TCAS. Mitigation by TCAS of STCA related hazards is not to be accounted for in setting target levels of safety.

The qualitative safety assessment followed the EUROCONTROL Safety Assessment Methodology (SAM) which consisted of preliminary identification of hazardous conditions. Errors and malfunctions related to the functioning of STCA, and the interoperability of STCA and TCAS were considered. Inputs to the assessment were ATC incidents from monitoring, analysis of STCA-TCAS control loops, workshop with operational expert, and analysis of existing studies.

C.3.4.2 Risk assessment & Derivation of candidate safety requirements

After the hazard identification, a risk assessment and mitigation was performed, as required by ESARR 4. An event tree analysis was used to determine quantitative safety objectives and then a fault tree analysis was used to derive quantitative safety requirements to meet those objectives.

An example of a safety objective is that an avoiding instruction by an ATCO received in an en-route airspace simultaneously to and incompatible with a TCAS RA occurs no more than 4 times a year at an ATC centre with 500,000 flights per year. An example of one of the candidate safety requirements is that the likelihood of having STCA out of service (complete) loss shall be less than 9 times a month at an ATC centre with 500,000 flight hours per year. The results of this generic safety assessment have to be reviewed at a local level (this point was emphasised during audience questioning).

C.4 PASS Phase 3: Synthesis and guidelines

The purpose of phase 3 of the PASS project was to consolidate main project outcomes by deriving candidate operational, safety and performance requirements and to summarise the work performed and disseminate outcomes in the ATM community.

C.4.1 Main study outcomes and lessons learnt

There is now a better understanding of STCA (and ACAS) operations in the current European environment. Elements were provided on RA downlink reliability and operational characteristics in the prospect of displaying down-linked ACAS RAs at controller working positions. The key factors influencing performance and safety aspects of STCA operations (including level of interaction with ACAS) have been identified: ANSP strategy; STCA parameters and optional features; Traffic and encounter characteristics; and Air traffic controller's intervention.

A comprehensive and re-useable framework for operational performance and safety assessment of joint STCA and ACAS operations has been delivered. The framework includes specifications for a set of models but the corresponding implementations were not developed to be re-used by third-parties (point emphasised during audience questioning). Performance metrics of STCA effectiveness identified are: likelihood, relevance and efficacy of STCA alerts, and level of STCA/TCAS interaction. A generic framework to assess hazards related to collision prevention by air traffic controllers assisted by STCA, including undesirable interaction with TCAS RAs, is available for re-use. The framework includes generic event-trees and fault trees to be reviewed at local level.

Using the generic framework, candidate operational, performance and safety requirements have been proposed to complement the EUROCONTROL specifications for STCA.

C.4.2 Project conclusions and recommendations

PASS studied performance and safety aspects of STCA operations including technical, procedural and human performance aspects and considerations of the interactions with TCAS.

Typical safety assessment methods show limitations when trying to provide a dynamic view of safety net issues, and need to be complemented by the model-based assessment methodology. PASS safety and performance assessment techniques are appropriate for ANSPs wanting to assure the safe use of STCA in their airspace, and for assessing the safety benefits brought by STCA in their airspace. PASS techniques would usefully complement the monitoring of an STCA system in operation, and aid the fine tuning of STCA system parameters and thresholds.

Clear definition and choice of ANSP's strategy are key for STCA effectiveness and to setting STCA performance targets. The more conservative strategies reduce the likelihood of undesired interaction between STCA and TCAS through provision of longer warning times. However, the more conservative strategies are less effective in keeping the number of nuisance alerts to an acceptable minimum level. Issues of overlapping STCA and TCAS alerts cannot be addressed simply by tuning the STCA parameters. All STCA configurations showed some degree of interaction with TCAS. Interaction may be limited if air traffic controllers use procedures and working methods adapted to the ANSP's strategy.

PASS work on safety assurance and safety benefit aspects of STCA operation should be reviewed in other arenas. EUROCONTROL SRC for aspects related to Safety Net regulation and SESAR programme for aspects related to research and development (R&D). The PASS framework on safety assurance and benefit aspects of STCA operation can largely be reused by other organisations. In the context of an ANSP implementing an STCA system, PASS generic safety and performance analyses are to be customised with local data and inputs.

The PASS framework should enable the investigation of the potential impact on STCA effectiveness of new concepts and potential changes to STCA. The realism of the PASS framework could be improved in order to lead to performance requirements reflecting more closely the performance of actual STCA systems. To progress on the definition of an overall operational concept of operations for compatible STCA and TCAS, controller and pilot in-the-loop simulations could be conducted to evaluate situational awareness and alert management, and further determine the influencing factors.

The PASS project recommends that ANSPs should perform operational monitoring of STCA and TCAS occurrences in their airspace in support to their STCA performance analysis. Candidate requirements should be promoted within the Safety net Performance Improvement Network Subgroup (SPIN-SG) and EUROCONTROL STCA specification & guidance material should be updated to include lessons learnt. Candidate requirements should be further consolidated and developed up to pre-operational stage in SESAR context. ANSPs implementing an STCA system should take into account the project conclusions depending on the strategy they adopt with regard to the operation and optimisation of their STCA system. A member of the audience noted that care should be taken when defining common requirements because for example measured performance may vary between ANSPs if different sized encounter envelopes are used.

C.5 Workshop conclusions

C.5.1 The future of safety nets in SESAR

From an operations perspective safety nets are addressed in the SESAR projects 4.8.1, 4.8.2 and 4.8.3. The technical counterparts of these projects are the SESAR projects 10.4.3, 9.47 and 15.4.3 respectively.

The PASS results are used in particular in the 4.8 projects. A limited amount of additional use of the encounter model-based methodology is planned to take place as well.

C.5.2 Chairman's main issues

In his closing remarks the workshop chairman raised a number of issues:

During the years since the Überlingen accident the awareness of important issues related to safety nets has significantly increased. However, the PASS monitoring activities showed that unclear situations are still happening. The reasons behind are not yet sufficiently understood and there is a need for further awareness creation.

Regarding some technical issues there is a need for action. For example, the cause of empty RA downlink messages needs to be understood and addressed.

The PASS project was initiated in a wider context than SESAR. The initiative should be continued in a wider context as well, possibly by moving it closer to operations.

The now existing encounter models should be capitalised on to the greatest extent possible. Ways and means to move further than the existing plans in SESAR should be explored.

C.6 Debriefing in the SPIN Sub-Group

A debriefing of the PASS dissemination workshop took place in the EUROCONTROL SPIN (Safety nets Performance Improvement Network) Sub-Group meeting that was conducted during the two days following the workshop.

The results of Phase 1, Monitoring, were generally considered valuable.

The results of Phase 2, European STCA Environment Modelling and Safety & Performance Analysis, were generally considered promising but a number of issues were identified:

a) The modelling has considered a generic environment and has not been validated in a specific environment. Consequently the analysis results have to be handled with care.

b) The encounter models are not released, which would be a prerequisite for further work. This is in particular an issue because no resources are available inside SESAR or the Agency to perform or commission further work using the existing encounter models. (Note that the encounter model specifications are released.)

c) There is a concern that the analysis results could start to live a life of their own anyhow. In particular the ongoing activities to bridge the current gap between SESAR and EASA (between R&D and Rule Making) could lead to unrealistic rules when the current quantitative analysis results would be used. A case in point is that the safety analysis considers eight outages of STCA per month acceptable from a safety point of view. But from an operational point of view this would be unacceptable because controllers would lose trust in STCA immediately which would render STCA useless.

d) Whilst the encounter models are not released, the detailed fault trees and event trees are released. However, any further use of these trees should start with a detailed review of the underlying assumptions in order to produce more realistic quantitative results.

The PASS project recommendation "ANSP should perform operational monitoring of STCA and TCAS occurrences in their airspace in support to their STCA performance analysis" was supported by the SPIN Sub-Group.

The PASS project recommendation "Candidate requirements should be promoted within SPIN-SG and EUROCONTROL STCA Specification & Guidance Material should be updated to include lessons learnt" was not supported by the SPIN Sub-Group. The candidate requirements were not considered mature enough. Nevertheless some of the lessons learnt could be used to improve the current STCA documentation. However, a prerequisite for this would be an agreed overall process.

The PASS project recommendation "Candidate requirements should be further consolidated and developed up to pre-operational stage in SESAR context" was supported by the SPIN Sub-Group, provided that sufficient validation activities will be undertaken.

The PASS project recommendation "ANSPs implementing an STCA system should take into account the project conclusions depending on the strategy they adopt with regard to the operation and

optimisation of their STCA system" was in principle supported by the SPIN Sub-Group, however the conclusions were considered being not sufficiently developed to be of practical use.

C.7 Overall conclusions and recommendations

C.7.1 Conclusions

The objectives of the PASS project have been achieved:

- Progress has been made towards standards for ground-based safety nets through quantified requirements for STCA by proposing candidate operational, safety and performance requirements; and
- Progress has been made with an overall concept of operation for ground-based and airborne safety nets, ensuring compatible STCA and TCAS operations.

The proposed candidate operational, safety and performance requirements now need to be refined to better reflect the complexity of the European core area. The refined requirements must be validated in a representative pre-operational environment.

Standards for STCA also contribute to ensuring compatible STCA and TCAS operations. Further progress in this area has been made by providing elements for decision-making regarding RA downlink. These elements have been highlighted in the October 2009 second RA downlink workshop and now assist in the concept development and validation work in SESAR project 4.8.3.

The work undertaken in the PASS project has addressed the 2007-2010 operational contexts. In the short term, SESAR step 1, no significant changes are expected. In the medium and long term, SESAR steps 2 and 3, significant changes will materialise and further work is needed to develop and validate requirements for future-proof safety nets.

The PASS project deliverables and the dissemination workshop presentations are available on the PASS web site:

http://www.eurocontrol.int/safety-nets/public/standard_page/PASS.html

C.7.1.1 Recommendations

a) The PASS results should be further developed and validated in SESAR.

b) The SPIN Sub-Group should continue to support the safety nets development work in SESAR.

- The following actions should be considered regarding SPIN Sub-Group support to refinement and validation of candidate operational, safety and performance requirements in SESAR:
    - Review the performance indicators that were used in the PASS project;
    - Determine how these performance indicators can be measured in a local context; and
    - Perform measurements in as many local environments as possible.

d) An agreed overall process should be established for incorporation of mature results of SESAR safety nets development work into existing EUROCONTROL specifications and guidance material.

e) Active awareness creation and promotion of best practices regarding safety nets should be continued.

C.8 Workshop participants

(*)denotes participation in the debriefing in the SPIN Sub-Group as well

1.(*)[redacted] skyguide (SWITZERLAND)

2.[redacted] INDRA Sistemas (SPAIN)

3.[redacted] Egis Avia (FRANCE)

4.[redacted] Rockwell Collins (FRANCE)

5.(*) [redacted] DSNA (FRANCE)
6.(*) [redacted] NAV Portugal (PORTUGAL)
7.(*) [redacted] EUROCONTROL (BELGIUM)
8. [redacted] SESAR JU (BELGIUM)
9.(*) [redacted] DFS (GERMANY)
10. [redacted] LPS SR (SLOVAKIA)
11. [redacted] Italian MOD Air Force (ITALY)
12. [redacted], Egis Avia (FRANCE)
13.(*) [redacted] EUROCONTROL EEC (FRANCE)
14. [redacted] Egis Avia (FRANCE)
15.(*) [redacted] EUROCONTROL (BELGIUM)
16. [redacted] DFS (GERMANY)
17. [redacted] LPS SR,s.p. (SLOVAKIA)
18. [redacted] DFS (GERMANY)
19. [redacted] EUROCONTROL (BELGIUM)
20.(*) [redacted] NAV Portugal (PORTUGAL)
21.(*) [redacted] Sakaeronavigatsia (GEORGIA)
22.(*) [redacted] LPS SR s. p. (SLOVAKIA)
23. [redacted] NLR (NETHERLANDS)
24. [redacted] Naviair (DENMARK)
25.(*) [redacted] QinetiQ (UK)
26.(*) [redacted] QinetiQ (UK)
27. [redacted] Sloveniacontrol Ltd (SLOVENIA)
28. [redacted] DFS (GERMANY)
29.(*) [redacted] DFS (GERMANY)
30.(*) [redacted] Sakaeronavigatsia (GEORGIA)
31. [redacted] Thales (FRANCE)
32. [redacted] LPS SR,s.p. (SLOVAKIA)
33. [redacted] DSNA (FRANCE)
34. [redacted] Malta Air Traffic Services (MALTA)
35. [redacted] DFS (GERMANY)
36. [redacted], EUROCONTROL (BELGIUM)
37. [redacted] GS-DETEC (SWITZERLAND)
38. [redacted] Deep Blue (ITALY)
39. [redacted], Sloveniacontrol Ltd (SLOVENIA)
40. [redacted] LPS SR,s.p. (SLOVAKIA)
41.(*) [redacted] Egis Avia (FRANCE)
42.(*) [redacted] TechnoSky Srl (ITALY)
43.(*) [redacted] NAV Portugal (PORTUGAL)

44.(*) [redacted] Deep Blue (ITALY)
45.(*) [redacted] DSNA (FRANCE)
46.(*) [redacted] EUROCONTROL EEC (FRANCE)
47.(*) [redacted] skyguide (SWITZERLAND)
48. [redacted] NLR (NETHERLANDS)
49. [redacted] MAA (UK)
50.(*) [redacted] Sakaeronavigatsia (GEORGIA)
51.(*) [redacted] Helios (UK)
52.(*) [redacted] Deep Blue (ITALY)
53. [redacted] EUROCONTROL MUAC (NETHERLANDS)
54.(*) [redacted] EUROCONTROL (BELGIUM)

Appendix D Example safety requirements

These quantitative safety requirements are based on a specific model airspace developed in the PASS project.

<table>
<tr><td>Identifier</td><td>REQ-PASS-SR-01</td></tr>
<tr><td>Requirement</td><td>The likelihood of an error in implementation of STCA parameter region shall be less than 9.7x10-5 per flight hour.</td></tr>
<tr><td></td><td>Correct implementation of STCA parameters for timeliness of alerts</td></tr>
<tr><td></td><td>(Based on PASS outcomes). The operational safety assessment (WA4) identified “Event 43’ ‘Error in implementation of STCA parameter region’” as a basic cause for several OHs with frequency values determined thanks to a top down approach applied to the fault trees. This basic event has the most stringent safety objective when involved in OH5. This basic event can be involved in all OHs.
<table>
<tr><th>Basic event</th><th>Frequency</th><th>Operational hazard</th></tr>
<tr><td rowspan="6">Event 43’ ‘Error in implementation of STCA parameter region causing late alert’</td><td>2.1x10-4 / flight hour</td><td>OH1: Lack of ATCO instruction to solve a short-term conflict</td></tr>
<tr><td>1.1x10-3 / flight hour</td><td>OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA</td></tr>
<tr><td>2.7x10-4 / flight hour</td><td>OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible</td></tr>
<tr><td>4.5x10-4 / flight hour</td><td>OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible</td></tr>
<tr><td>9.7x10-5 / flight hour</td><td>OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible</td></tr>
<tr><td>2.9x10-4 / flight hour</td><td>OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible</td></tr>
</table></td></tr>
</table>

		ECTRL-STCA-02, ECTRL-SCTA-06, ECTRL-STCA-07, ECTRL-SCTA-08, ECTRL-STCA-12	

<table>
<tr><td>Identifier</td><td>REQ-PASS-SR-02</td></tr>
<tr><td>Requirement</td><td>The likelihood of a lack of STCA alert due to tight parameters setting (‘success case’) shall be less than 2.1x10-4 per flight hour.</td></tr>
<tr><td></td><td>Adequate definition of STCA parameters for issuance of alerts</td></tr>
<tr><td></td><td>(Based on PASS outcomes). The operational safety assessment (WA4) identified “Event 56 ‘Lack of STCA alert due to tight parameters setting (success case)’“ as a basic cause for several OHs with frequency values determined thanks to a top down approach applied to the fault trees. This basic event has the most stringent safety objective when involved in OH1. This basic event can be involved in all six OHs.
<table>
<tr><th>Basic event</th><th>Frequency</th><th>Operational hazard</th></tr>
<tr><td rowspan="5">Event 56 ‘Lack of STCA alert due to tight parameters setting (success case)’</td><td>2.1x10-4 / flight hour</td><td>OH1: Lack of ATCO instruction to solve a short-term conflict</td></tr>
<tr><td>2.3x10-2 / flight hour</td><td>OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA</td></tr>
<tr><td>5.4x10-3 / flight hour</td><td>OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible</td></tr>
<tr><td>9.0x10-3 / flight hour</td><td>OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible</td></tr>
<tr><td>1.9x10-3 / flight hour</td><td>OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible</td></tr>
</table></td></tr>
</table>

			5.9x10-3 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible	

		ECTRL-STCA-02, ECTRL-SCTA-06, ECTRL-STCA-07, ECTRL-SCTA-08, ECTRL-STCA-12	

Identifier	REQ-PASS-SR-03
Requirement	The likelihood of a lack of STCA alert due to tight parameters setting ('success case') shall be less than 2.1x10-4 per flight hour.
	The likelihood of having STCA out of service shall be less than 2.1x10-4 per flight hour.

(Based on PASS outcomes). The operational safety assessment (WA4) identified "STCA LOSS 'STCA out of service'" as a basic cause for several OHs with frequency values determined thanks to a top down approach applied to the fault trees. This basic event has the most stringent safety objective when involved in OH1. This basic event can be involved in all six OHs.

Basic event	Frequency	Operational hazard
STCA LOSS 'STCA out of service'	2.1x10-4 / flight hour	OH1: Lack of ATCO instruction to solve a short-term conflict
	2.3x10-2 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
	5.4x10-3 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
	9.0x10-3 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
	1.9x10-3 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
	5.9x10-3 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

		ECTRL-STCA-02, ECTRL-SCTA-16

Identifier	REQ-PASS-SR-04
Requirement	The likelihood of an excessive nuisance STCA alert rate shall be less than 1.2x10-3 per flight hour.

(Based on PASS outcomes).
The operational safety assessment (WA4) identified "STCA – NUISANCE 'Excessive nuisance STCA alert rate'" as a basic cause for several OHs with frequency values determined thanks to a top down approach applied to the fault trees. This basic event has the most stringent safety objective when involved in OH1. This basic event can be involved in all six OHs.

Basic event	Frequency	Operational hazard
STCA – NUISANCE 'Excessive nuisance STCA alert rate'	1.2x10-3 / flight hour	OH1: Lack of ATCO instruction to solve a short-term conflict
	3.7x10-2 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
	8.7x10-3 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
	1.5x10-2 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
	3.0x10-3 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA

			and incompatible
		9.7x10-2 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Identifier	REQ-PASS-SR-05		
Requirement	The likelihood of an excessive false STCA alert rate shall be less than 1.2x10-3 per flight hour.		
	Basic event	Frequency	Operational hazard
	STCA – FALSE 'Excessive false STCA alert rate'	1.2x10-3 / flight hour	OH1: Lack of ATCO instruction to solve a short-term conflict
		3.7x10-2 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
		8.7x10-3 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
		1.5x10-2 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
		3.0x10-3 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
		9.7x10-2 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Identifier	REQ-PASS-SR-06		
Requirement	The likelihood of that a SSR code / flight ID is erroneously inserted in the suppression list of STCA shall be less than 2.1x10-4 per flight hour.		
	Basic event	Frequency	Operational hazard
	Event 25 SSR code / flight ID erroneously inserted in the suppression list of STCA	2.1x10-4 / flight hour	OH1: Lack of ATCO instruction to solve a short-term conflict
		2.3x10-2 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
		5.4x10-3 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
		9.0x10-3 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
		1.9x10-3 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
		5.9x10-3 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Identifier	REQ-PASS-SR-07		
Requirement	The likelihood of an erroneous design of STCA algorithm shall be less than 9.7x10-5 per flight hour.		
	Basic event	Frequency	Operational hazard
	Event 27 'Erroneous design of STCA algorithm'	2.1x10-4 / flight hour	OH1: Lack of ATCO instruction to solve a short-term conflict
		1.1x10-3 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
		2.7x10-4 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a

			TCAS RA and incompatible
		4.5x10-4 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
		9.7x10-5 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
		2.9x10-4 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Identifier	REQ-PASS-SR-08		
Requirement	The likelihood of a late STCA alert is issued due to erroneous parameters setting shall be less than 9.7x10-5 per flight hour.		
	Basic event	Frequency	Operational hazard
	Event 37 'Late STCA alert due to erroneous parameters setting'	1.1x10-3 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
		2.7x10-4 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
		4.5x10-5 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
		9.7x10-5 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
		2.9x10-4 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Identifier	REQ-PASS-SR-09		
Requirement	The likelihood of a late STCA alert is issued due to tight parameters setting ('success case') shall be less than 9.7x10-5 per flight hour.		
	Basic event	Frequency	Operational hazard
	Event 39 Late STCA alert due to tight parameters setting (success case)	1.1x10-3 / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
		2.7x10-4 / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
		4.5x10-5 / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
		9.7x10-5 / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
		2.9x10-4 / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

Appendix E Example performance requirements

The performance requirements proposed in this section are derived from the PASS study outcomes and result from the model-based performance evaluation that has been conducted. In order to give an insight into the rationale that led to the definition of these performance requirements, Table 3 provides the mapping that has been defined between STCA strategies and STCA families, for both TMA and en-route airspace. This information is complemented by Table 4, which provides the STCA parameters that have proved to most affect STCA performance (i.e. separation thresholds and warning time).

	TMA airspace	En-route airspace
Liberal strategy	very_last_mn about_very_last_mn	very_last_mn beyond_last_mn
Intermediate strategy	beyond_last_mn nearby_last_mn	almost_last_mn
Conservative strategy		before_last_mn last_two_mns

Table 3 Mapping between STCA strategies and STCA Families

	STCA family	Lateral threshold	Vertical threshold	Warning time
TMA	Very_last_mn	1.5 NM	500 ft	40 s
	About_very_last_mn	2 NM	500 ft	60 s
	Beyond_last_mn	2.9 NM	725 ft	40 s
	Nearby_last_mn	3 NM	740 ft	50 s
En-route	Very_last_mn	2.5 NM	500 ft	55 s
	Beyond_last_mn	3.7 NM	700 ft	55 s
	Almost_last_mn	4.9 NM	750 ft	70 s
	Before_last_mn	4.9 NM	800 ft	90 s
	Last_two_mnx	5 NM	800 ft	120 s

Table 4 Main STCA parameters for TMA and en-route airspace

Identifier	REQ-PASS-PR-01
Requirement	When a liberal strategy is favoured, STCA ***shall*** alert initially “major”, or worse, separation infringements (i.e. conflicts where less than 50% of the applicable separation minima would remain without the effect of any controller’s avoiding instruction); When a intermediate strategy is favoured, STCA ***shall*** alert initially “significant”, or worse, separation infringements (i.e. conflicts where less than 80% of the applicable separation minima would remain without the effect of any controller’s avoiding instruction); When a conservative strategy is favoured, STCA ***shall*** alert initially separation infringements (i.e. conflicts where less than the applicable separation minima would remain without the effect of any controller’s avoiding instruction). *Note: Operationally relevant conflicts to be alerted by STCA depend on the rule set and optimisation strategy favoured by the local ANSP:* *When a liberal strategy is favoured, STCA are primarily designed to make a significant positive contribution to the effectiveness of collision prevention essentially.* *When an intermediate strategy is favoured, STCA are primarily designed to*

	make a substantial positive contribution to the effectiveness of both separation protection and collision prevention. *When a conservative strategy is favoured, STCA are primarily designed to make an extensive positive contribution to the effectiveness of separation protection (and consequently to collision prevention).* *Note: The conflicts considered are those involving controlled flights to which ATC is expected to provide separation in the volume of airspace (e.g. IFR/VFR in class D or IFR/IFR in class E). For these conflicts, an initial separation infringement is a situation where an infringement would occur in the absence of any controller's avoiding instruction to maintain or restore separation.*
	(Based on PASS outcomes): The model-based performance evaluation (WA2) demonstrated that: a) "the en-route very_last_mn and beyond_last_mn STCA configurations, as well as the TMA very_last_mn and about_very_last_mn STCA configurations, appear focused on the provision of alerts for conflicts with an SC1 or SC2 initial severity (i.e. encounter severity without controller intervention). These two severity classes are defined as a separation less than 50% of applicable ATC minima." ([W168]) b) "the en-route almost_last_mn STCA configuration, as well as the TMA beyond_last_mn and nearby_last_mn STCA configurations, appears focused on the provision of alerts for conflicts with an SC1 to SC3 initial severity (i.e. encounter severity without controller intervention). These three severity classes are defined as a separation less than 80% of applicable ATC minima." ([W168]) c) "the en-route before_last_mn and last_two_mns STCA configurations appear focused on the provision of alerts for conflicts with an SC1 to SC4 initial severity (i.e. encounter severity without controller intervention). These four severity classes are defined as a separation less than the applicable ATC minima." ([W168])

Identifier	REQ-PASS-PR-02
Requirement	When a liberal strategy is favoured, STCA ***shall*** produce alerts for at least 95% of initially "major", or worse, separation infringements; When a intermediate strategy is favoured, STCA ***shall*** produce alerts for at least 95% of initially "major", or worse, separation infringements, and for at least 80% of initially "significant" separation infringements; When a conservative strategy is favoured, STCA ***shall*** produce alerts for at least 95% of initially "major", or worse, separation infringements, for at least 80% of initially "significant" separation infringements, and for at least 50% of initially "minor" separation infringements.
	(Based on PASS outcomes**):** The model-based performance evaluation (WA2) demonstrated that: The en-route *very_last_mn* and *beyond_last_mn* STCA configurations, as well as the TMA *very_last_mn* and *about_very_last_mn* STCA configurations, are able to produce alerts in more than 95% of conflicts with an SC1 or SC2 initial severity (i.e. conflict severity without avoiding instruction). ([W168]) The en-route *almost_last_mn* STCA configuration, as well as the TMA *beyond_last_mn* and *nearby_last_mn* STCA configurations, are able to produce alerts in more than 95% of conflicts with an SC1 or SC2 initial severity (i.e. conflict severity without controller avoiding instruction), and in more than 80% of conflicts with an SC3 initial severity. ([W168]) The en-route *before_last_mn* and *last_two_mns* STCA configurations are able to produce alerts in more than 95% of conflicts with an SC1 or SC2 initial severity

	(i.e. conflict severity without controller avoiding instruction), in more than 80% of conflicts with an SC3 initial severity and in more than 50% of conflicts with an initial SC4 severity. ([W168])

Identifier	REQ-PASS-PR-03
Requirement	When a liberal strategy is favoured, STCA ***shall*** produce alerts in less than 80% of situations with an initially "significant" or "minor" separation infringement, or with no initial separation infringement; When a intermediate strategy is favoured, STCA ***shall*** produce alerts in less than 80% of situations with an initially "minor" separation infringement or no initial separation infringement; When a conservative strategy is favoured, STCA ***shall*** produce alerts in less than 80% of situations with no initial separation infringement.

Identifier	REQ-PASS-PR-04
Requirement	When a liberal strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of conflicts with an initially "serious" separation infringement and 80% of conflicts with an initially "major" separation infringement, assuming a timely and appropriate controller's reaction; When a intermediate strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of conflicts with an initially "major", or worse, separation infringement and 80% of conflicts with an initially "significant" separation infringement, assuming a timely and appropriate controller's reaction; When a conservative strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of conflicts with an initially "major", or worse, separation infringement, 80% of conflicts with an initially "significant" separation infringement and 50% of conflicts with an initially "minor" separation infringement, assuming a timely and appropriate controller's reaction.

Identifier	REQ-PASS-PR-05
Requirement	a) When a liberal strategy is favoured, the proportion of alerts produced less than 20 seconds before an initially "major", or worse, separation infringement shall be less than 20%; b) When a intermediate strategy is favoured, the proportion of alerts produced less than 20 seconds before an initially "significant", or worse, separation infringement shall be less than 20%; c) When a conservative strategy is favoured, the proportion of alerts produced less than 20 seconds before an initially "minor", or worse, separation infringement shall be less than 20%.

Identifier	REQ-PASS-PR-06
Requirement	When a liberal strategy is favoured, STCA ***shall*** produce less than 20% of alerts with a duration less than 20 seconds in initially "major", or worse, separation infringements; When a intermediate strategy is favoured, STCA ***shall*** produce less than 20% of alerts with a duration less than 20 seconds in initially "significant", or worse, separation infringements; When a conservative strategy is favoured, STCA ***shall*** produce less than 20% of alerts with a duration less than 20 seconds in initially "minor", or worse, separation infringements.

- **END OF DOCUMENT -**