PASS Final report – Synthesis and Guidelines

Performance and safety Aspects of Short-term Conflict Alert – full Study

PASS Project

Drafted by: Christian Aveneau, Hervé Drévillon & Béatrice Raynaud

Authorised by: Thierry Arino on 17/11/2010

ADDRESSEES:	COPY TO:
Stan Drozdowski (EUROCONTROL), Ben Bakker (EUROCONTROL), Bernard Brunner (EUROCONTROL), Garfield Dean (EUROCONTROL) Christopher Shaw (EUROCONTROL) Hans Wagemans (EUROCONTROL) John Law (EUROCONTROL)	DSNA Participants, Deep Blue Participants, QinetiQ Participants, Egis Avia Participants.

RECORD OF CHANGES

Issue	Date	Detail of changes
0.1	15-10-2010	Document initialisation
0.2	25-10-2010	Material added in chapters 1 to 5 and Appendix A
0.3	26-10-2010	Editorial changes
0.4	10-11-2010	Changes to all sections following review performed at close-out meeting
1.0	12-11-2010	First version delivered to EUROCONTROL
1.1	17-11-2010	Revised version following comments from EUROCONTROL and QinetiQ

IMPORTANT NOTE: ANY NEW VERSION SUPERSEDES THE PRECEDING VERSION, WHICH MUST BE DESTROYED OR CLEARLY MARKED ON THE FRONT PAGE WITH THE MENTION *OBSOLETE VERSION*

EXECUTIVE SUMMARY

E.1. Background, scope and objectives

E.1.1. In the context of Short-Term Conflict Alert harmonisation and evolution in Europe, EUROCONTROL (European organisation for the safety of air navigation) launched the PASS project (**P**erformance and safety **A**spects of **S**hort-term Conflict Alert – full **S**tudy). It was undertaken based on the recommendations of the EUROCONTROL FARADS (Feasibility of ACAS (Airborne Collision Avoidance System) RA (Resolution Advisory) Downlink Study) and of the ACAS-STCA workshop held on 27th and 28th March 2007 in Dübendorf, Switzerland, that aimed at addressing, discussing and understanding all relevant issues and problem areas related to STCA, ACAS and the interactions between them.

E.1.2. The purpose of the project was to study performance and safety aspects of STCA operations, including technical, procedural, and human performance issues and considerations of the interactions with ACAS. The project aimed at defining quantified safety and performance requirements for STCA and progressing with an overall concept of operations for compatible STCA and ACAS operations.

E.1.3. The project falls within the scope of the EUROCONTROL SPIN (Safety Nets Performance Improvement Network) Sub-Group and originates from the positive conclusions of a feasibility study conducted in 2006 within Activity Field 4 (System Safety Defences) of the EUROCONTROL European Safety Programme. In the context of SPIN, EUROCONTROL has commenced the standardisation of ground-based safety nets and, in particular, has developed the EUROCONTROL Specification for STCA and the accompanying EUROCONTROL Guidance Material for STCA. The PASS project was launched to progress the definition of quantified safety and performance requirements for STCA, as well as the definition of a consistent overall concept for ground-based and airborne safety nets.

E.1.4. The project has been an early contribution to the evolution of ground-based and airborne safety nets towards performance-oriented ATM operations in the context of the Single European Sky ATM Research Programme (SESAR).

E.2. Operational monitoring of STCA and ACAS operations

E.2.1. Firstly, a monitoring framework was developed, defining the types of safety-net related occurrences that would be of interest, the participation asked from external partners, the inputs needed for each safety-net related occurrence, the data that would be extracted from these inputs and the metrics that would be computed for the whole set or some subsets of the safety-net related occurrences.

E.2.2. Safety-net related occurrences of interest were gathered from several States, with different STCA implementations. Three Air Navigation Service Providers (ANSPs), French DSNA, Swiss skyguide and German DFS, participated in the gathering of operational data on occurrences of interest. Other safety-net related occurrences of interest were extracted from public sources from the following countries: the United Kingdom, Denmark, the Czech Republic, Ireland and Estonia.

E.2.3. These occurrences were analysed statistically to provide a descriptive view focused on elementary events (STCA and ACAS alerts, pilot and controller actions and reactions, significant points). A complementary study highlighted the timing and quality of pilot ACAS reports. These analyses provided a better understanding of the typical sequence of events during Air Traffic Management (ATM) safety occurrences in which STCA and/or ACAS played a role, and of the factors that have a major influence on this sequence. The monitoring also analysed RA downlink data, leading to quantified results about the quality and reliability of RA downlink data.

E.2.4. Based on the outputs of the project monitoring activities, several approaches to the use of STCA have been identified and categorized, taking into consideration the differences of these approaches with the scope of ACAS. Each ANSP's strategy with regard to STCA operation and optimisation guides the choice of the system's parameter values towards more time-critical or less time-critical values and smaller or larger values for separation thresholds. Five distinct STCA families have thus been identified in en-route airspace and four in Terminal control Area (TMA) airspace.

E.3. Model-based operational performance assessment of STCA and ACAS operations

E.3.1. Performance assessment of STCA and ACAS has been conducted using a set of models that simulates STCA systems, their environment and operational use as observed during the project monitoring activities.

E.3.2. These models include an encounter model of operationally realistic situations in which STCA and ACAS might be involved, built from the observed properties of relevant conflicts in European radar recordings. The behaviour of STCA systems in these conflicts has been reproduced through an STCA model implementing the EUROCONTROL Reference STCA System Specification. The Communications, Navigation and Surveillance (CNS) environment in which STCA is operated is also taken into account, notably with a model of Air Traffic Control (ATC) surveillance. Lastly, the responses brought by human actors to safety nets alerts have been implemented in specific controller and pilot models.

E.3.3. The safety benefit aspects of STCA and ACAS operations were assessed by conducting model-based simulations using this framework in a series of operationally realistic simulation scenarios. Three such sets of operational scenarios were used:

- Basic scenarios in order to determine the parameters having the most significant impact on STCA performance;
- Scenarios covering a wide range of realistic STCA implementations, with common CNS features and human actors behaviour, to investigate the influence of STCA parameters and optional features; and
- Specific scenarios for sensitivity analyses of the environmental and human factors possibly affecting STCA performance.

E.3.4. In parallel with setting up the model-based simulations, a set of metrics has been defined that allows the quantification of STCA performance in any given operational scenario. These metrics relate to the likelihood of STCA alerts, their operational relevance, their operational efficacy, and the compatibility with ACAS. At their core, these metrics use a definition of the initial conflict severity, which is a measure of the extent of the loss of separation in the absence of human intervention.

E.3.5. The computation of these performance metrics, through model-based simulations over the different operational scenarios, allowed the characterisation in more depth of the alternative strategies that ANSPs might follow when implementing and optimising their STCA system. The following three strategies have been identified:

- A liberal strategy in favour of an STCA primarily designed to make a significant contribution to the effectiveness of collision prevention (yet limited contribution to separation protection) by alerting the controller of only potentially major separation infringements and consequently fairly effective in reducing the likelihood of alerts in case of conflicts with less significant separation infringements;
- An intermediate strategy in favour of an STCA primarily designed to make a substantial contribution to the effectiveness of both separation protection and collision prevention by alerting the controller of potentially significant separation infringements, with a proportion of unnecessary alerts in case of conflicts without separation infringement or with minor separation infringements;
- A conservative strategy in favour of an STCA primarily designed to make an extensive contribution to the effectiveness of separation protection (and consequently to collision prevention) by alerting the controller of any separation infringements, with a proportion of unnecessary alerts in case of encounters without separation infringement.

E.3.6. The simulation results also highlighted that the notions of genuine, missed and nuisance alerts are likely to depend on the ANSP strategies for collision avoidance through respectively limited, substantial or extensive separation protection.

E.3.7. The results of the model-based performance evaluation, weighed against the high-level operational requirements defined in EUROCONTROL's Specification for STCA, allowed the quantification of performance requirements that should be met during nominal STCA operation. Because this performance assessment has been conducted on a generic airspace rather than on a specific one, they are proposed as candidate requirements against which the performance of operational STCA systems can be assessed.

E.4. Operational safety assessment of STCA and ACAS operations

E.4.1. A number of methodologies have been proposed as acceptable means of compliance with the provisions of ESARR 4 (EUROCONTROL Safety Regulatory Requirement for risk assessment and mitigation in ATM). Among these is EUROCONTROL's Air Navigation System Safety Assessment Methodology which has been used in the present study. Using this methodology, the operational safety assessment process derives safety requirements by considering unique operational hazards introduced by STCA or existing hazards that an STCA system might adversely affect. These hazards are examined in order to control their likelihood and their effects.

E.4.2. A preliminary hazard identification first found the potential errors and malfunctions of the ATM system which are related to the operation of STCA or to the interoperability of STCA and ACAS. This qualitative analysis was based on ATC incidents observed during the project monitoring and integrated inputs from other studies. Using this preliminary list of operational hazards, a quantitative event-tree analysis was performed to derive preliminary safety objectives, as required by ESARR 4. Safety objectives limit the frequency of occurrence of hazards, such that the associated risk would be acceptable.

E.4.3. In a subsequent step, the whole process was repeated to reach a consolidated list of operational hazards using expert judgment, analysis of other ACAS-related studies and a deeper understanding of cognitive aspects of the human actors' performance. A consolidated event-tree analysis of these hazards was performed to derive refined safety objectives. Finally, a quantitative fault-tree analysis evaluated the possible (human and system) failure modes leading to these consolidated hazards and enabled the derivation of safety requirements for STCA.

E.4.4. This last step permitted to share the safety objectives between the different causes of a given operational hazard. The most stringent frequency assigned to the basic causes related to each hazard was retained to define safety requirements. It is important to note that all derived safety requirements are generic and that they are based on conservative assumptions on human errors, external event occurrences and STCA configuration. To develop local safety requirements addressing specific ANSP needs, this safety assessment should be customised with local ANSP data.

E.5. Conclusions and recommendations

E.5.1. The project has studied performance and safety aspects of STCA operations, including technical, procedural and human performance issues, as well as considerations of the interactions with ACAS. The performance and safety investigations were concluded by the development of candidate operational, performance and safety requirements for STCA and STCA/ACAS compatibility. The work conducted also contributes to the definition of an overall concept of operations for STCA and ACAS.

E.5.2. The workshop on STCA & ACAS interaction and interoperability held on 27th and 28th March 2007 in Dübendorf raised a number of then unanswered questions which the PASS project has been able, at least partially, to answer. It notably shows that the issue of overlapping STCA and ACAS alerts can not be addressed simply by tuning the STCA parameters, as all the STCA configurations investigated showed some degree of interaction with ACAS. This interaction can however be limited if controllers use procedures that are adapted to the ANSP's strategy with regard to STCA implementation and optimisation.

E.5.3. The work conducted within the project highlighted the need for ANSPs to choose and clearly define a strategy with regard to the implementation and optimisation of their STCA system. This strategy is key for the effectiveness of STCA in their airspace and for the setting up of appropriate performance targets, including those related to interaction with TCAS.

E.5.4. Based on the project conclusions, it is recommended that ANSPs conduct operational monitoring of STCA and TCAS occurrences in their airspace so that STCA performance analysis includes the level of interaction with TCAS

E.5.5. It is recommended that the candidate operational, safety and performance requirements proposed by the project be promoted within the context of the SPIN Sub-Group and, that the EUROCONTROL STCA specification and guidance material be updated to include lessons learnt in this work.

E.5.6. It is recommended that the candidate requirements be further consolidated and developed up to pre-operational stage in the context of SESAR.

E.5.7. It is recommended that ANSPs implementing an STCA system take into account the project conclusions and recommendations that apply to the strategy used in the operation and optimisation of their system, especially those related to the STCA and ACAS interaction.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Introduction

1.1. Study scope and objectives

1.1.1. In the context of Short-Term Conflict Alert (STCA) harmonisation and evolution in Europe, EUROCONTROL launched the PASS project (**P**erformance and safety **A**spects of **S**hort-term Conflict Alert – full **S**tudy).

1.1.2. The purpose of the project was to study performance and safety aspects of STCA operations, including technical, procedural, and human performance aspects and considerations of the interactions with the Airborne Collision Avoidance System (ACAS). The project aims at defining quantified safety and performance requirements for STCA and progressing with an overall concept of operations for compatible STCA and Traffic alert and Collision Avoidance System (TCAS)[1] operations.

1.1.3. The PASS project ([D01]) was divided into three main phases, as follows:

- Phase 1: Monitoring & understanding of current situation;
- Phase 2: European STCA environment modelling & safety and performance analysis; and
- Phase 3: Enhanced modelling and analysis, synthesis and guidelines.

1.1.4. The monitoring activities conducted in Phase 1 of the project (October 2007 – April 2009) provided a better understanding of the typical sequence of events during Air Traffic Management (ATM) safety occurrences in which STCA and/or TCAS played a role, and of the factors that have a major influence on this sequence.

1.1.5. Based on the Phase 1 monitoring outcomes, Phase 2 of the project (November 2008 – December 2009) progressed on the modelling and analysis of joint STCA and TCAS operations. Both the performance aspects (in terms of safety benefits) and the safety assurance aspects (in terms of safety hazards) of STCA operations were investigated while taking into account the effect of ACAS operations. This investigation was completed and finalised during Phase 3 of the project (January 2010-November 2010), which was concluded by the development of candidate operational, safety and performance requirements for STCA and STCA / TCAS interoperability. The project has been acknowledged as an early contribution to the evolution of ground-based and airborne safety nets towards performance-oriented ATM operations in the context of the Single European Sky ATM Research Programme (SESAR).

1.1.6. The project outcomes are of particular interest for Air Navigation Service Providers (ANSP), national aviation authorities, ATM industry companies, SESAR, and other bodies contributing to ATM safety improvement, management and monitoring in Europe.

---

[1] TCAS is aircraft equipment that is an implementation of an ACAS. Hereafter, TCAS refers to TCAS II – the only equipment so far that is compliant with the ACAS II standard.

1.2. Background and context of the PASS project

Genesis of the project

1.2.1. The PASS project was undertaken based on the recommendations of the EUROCONTROL RA downlink study ([FARADS] project) and the ACAS-STCA workshop held on 27th and 28th March 2007 in Dübendorf ([WKS2007]). The FARADS project has investigated the technical feasibility and operational usefulness of presenting down-linked RAs to controllers as a potential means for understanding and managing the implications of TCAS for ATC. The Dübendorf workshop was set up jointly by EUROCONTROL and the Swiss Federal Department of the Environment, Transport, Energy and Communication (DETEC) to address, discuss and understand all relevant issues and problem areas related to STCA, ACAS and the interactions between them. It concluded on the interaction issue by a number of then unanswered questions:

- Can STCA be “tuned” to prevent issuance of RAs (Resolution Advisories)?
- Is STCA effective in case of imminent (or actual) separation infringements?
- Can STCA and ACAS be coordinated at system level?
- Is training sufficient enough to ensure appropriate pilot reaction to RAs?
- Can procedures and working methods for controllers be developed to limit interaction with possible RAs?
- Is pilot report of RAs effective enough to prevent disruptive ATC intervention?
- Can RA downlink help?
- Is training sufficient enough to ensure appropriate controller behaviour in case of ACAS/STCA events
- Which level of training on unusual situations is required for controllers?

1.2.2. The PASS project falls within the scope of the SPIN (Safety nets Performance Improvement Network) and originates from the positive conclusions of a feasibility study ([IAMSAFE]) conducted in 2006 within Activity Field 4 (System Safety Defences) of the European Safety Programme. The SPIN Task Force has commenced the standardization of ground-based safety nets and, in particular, has developed the EUROCONTROL Specification for STCA and the accompanying EUROCONTROL Guidance Material for STCA ([EGM20]). The PASS project was launched to progress the definition of quantified safety and performance requirements for STCA, as well as the definition of a consistent overall concept for ground-based and airborne Safety Nets (SNET).

1.2.3. While in execution, the project became an early contribution to the SESAR projects dealing with the evolution of ground-based and airborne safety nets ([P481], [P483]). The main goal of SESAR project 4.8.1 ([P481]) is to conduct appropriate evolution of ground-based safety nets to ensure that they will continue to play an important role as a last ATC safety layer against the risk of collision during future trajectory and separation operations. In addition SESAR project 4.8.3 ([P483]) will ensure that airborne and ground-based safety nets remain compatible in the changing ATM environment. During the initiation phase of both projects (in 2009), the PASS project of EUROCONTROL has been recognised as an early contribution to the SESAR work programme on safety nets expected to lay the foundations for the safety & performance evaluation of airborne and ground-based SNET operations to be conducted in the SESAR projects 4.8.1 and 4.8.3.

Background on STCA harmonisation in Europe

1.2.4. In Europe, a major milestone has been achieved to ensure the effectiveness of ground-based safety nets with the release by EUROCONTROL of specifications and supporting guidance material ([ES11], [EGM20]).

1.2.5. The EUROCONTROL Specification for STCA ([ES11]) describes the operational context in which STCA is intended to be used and specifies the minimum high-level requirements for the development, configuration and use of an STCA system. These requirements are derived from an analysis of the operational concept behind STCA systems, taking into account human performance, design, technical and safety aspects. They constitute the foundations for the more detailed operational, safety and performance requirements derived in the present study.

1.2.6. The EUROCONTROL Guidance Material, and in particular that related to the Reference STCA System (see Appendix A of [EGM20]) and to the Outline Safety Case for STCA System (see Appendix B-3 of [EGM20]), constitutes other key inputs of the performance and safety analyses conducted within the PASS project.

Building on the experience from the ACAS field

1.2.7. The present study also builds upon the experience gained, and the encounter model-based methodology used, in the standardisation of the performance of the airborne safety-net, i.e. ACAS. The ICAO 'Standards And Recommended Practices' (SARPs) for ACAS ([ACAS]) define a set of target 'risk ratios[2]' for different scenarios of aircraft equipage in a hypothetical airspace described by a 'safety encounter model'. ICAO also defines an 'ATM encounter model' which enlarges the scope of the featured encounters and which is used to standardise ATM compatibility requirements for ACAS through the definition of target levels of nuisance alerts and the deviations caused by responding to RAs.

[2] A 'risk ratio' compares the risk of a 'Near Mid-Air Collision' (NMAC) both with and without ACAS. Any risk ratio that is less than unity indicates that the deployment of ACAS II reduces the risk of collision and thus provides a safety benefit.

1.2.8. As the encounter models specified in the ICAO SARPs are not representative of any particular airspace, EUROCONTROL sponsored the “ACAS Analysis” (ACASA) project in 1998 to 2001. This project notably developed a European safety encounter model representative of actual operations at that time, which was a cornerstone in the establishment of the European ACAS mandate. This European safety encounter model was subsequently updated in the EUROCONTROL “ACAS Safety Analysis – post-RVSM (Reduced Vertical Separation Minima) Project” (ASARP) study, between 2003 and 2005, following the introduction of RVSM in European airspace. The encounter model-based methodology has also been used in forward looking studies that aimed at assessing the safety and operational performance of ACAS in novel ATM operations. From 2002 to 2005, the “Implications on ACAS Performances due to ASAS Implementation” (IAPA) project notably implemented a European ATM encounter model to support the analysis of the possible interaction between ACAS and future airborne separation operations.

1.2.9. The applicability and usefulness of the encounter model-based methodology for establishing quantified performance requirements for STCA was investigated in the “IAPA – ASARP Methodology for Safety net Assessment – Feasibility Evaluation” (I-AM-SAFE) project of EUROCONTROL ([IAMSAFE]). The methodology was demonstrated to be applicable and useful to evaluate the performance of STCA, and the possible interaction issues with ACAS, although some adaptations would be required to specifically address STCA. The present study developed a comprehensive model-based evaluation framework of STCA and ACAS operations building on the conclusions and recommendations of the I-AM-SAFE project.

1.3. Overview of the PASS Study

1.3.1. The PASS project ([D01]) consisted of several Work Areas (WA) that span the three project phases. The technical work was carried out by a consortium of four organisations (Deep Blue[3], DSNA[4], Egis Avia[5] and QinetiQ[6]) under the management of the Surveillance Separation & Safety (SSS) skill unit of Egis Avia.

Monitoring activity

1.3.2. Within Phase 1, **a first Work Area (WA1) aimed at providing a better understanding of the typical sequence of events in ATM occurrences in which STCA and/or TCAS played a role and of the factors that have a major influence on this sequence**. As illustrated in Figure 1, this was achieved through the analysis of a significant number (180) of ATC occurrences where an STCA alert and/or a TCAS alert triggered.

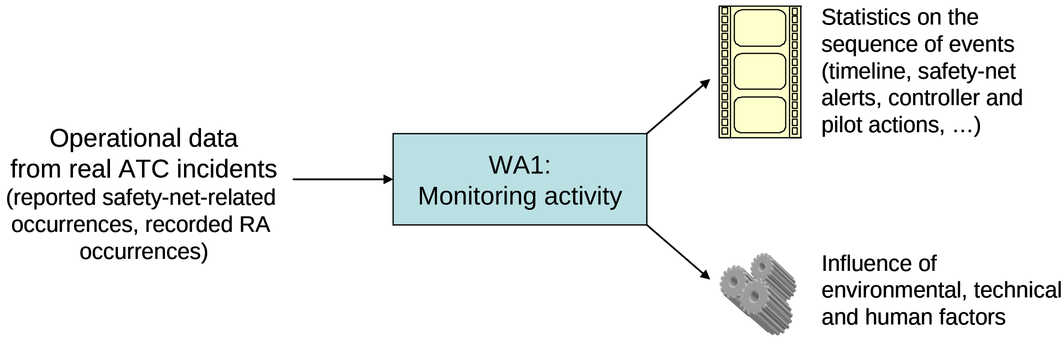


Figure 1: Monitoring & understanding of current situation (Work Area 1)

1.3.3. This monitoring activity covered as wide an airspace as possible in order to reflect different types of ATC operations. This was enabled by the involvement of DSNA in the PASS project team (and the access to its ATM data-recording infrastructure including an incident data-base and Mode S radar recordings), the specific contribution of DFS and skyguide (which granted access to radar recordings and reported occurrence reports), and the indirect contribution of other European Air Navigation Service Providers (through occurrence reports available in the public domain).

---

[3] Deep Blue is a research and consultancy company located in Italy with human factors and safety specialists involved in several international collaborative European projects. Website: http://www.dblue.it

[4] The 'Air Navigation Services Department' (DSNA) is part of the French civil aviation and provides air navigation services in the French airspace, as well as in the French overseas territories airspace. Website: http://www.dsna-dti.aviation-civile.gouv.fr

[5] Egis Avia is an engineering and consulting company in the fields of airport, ATM and air transport industry. Its clients include EUROCONTROL, national ANSPs, civil aviation administrations and industry. Website: http://www.egis-avia.com/

[6] QinetiQ is a science and technology organisation involved in ATM research for bodies such as UK Ministry of Defence, EUROCONTROL and national ANSPs. Website: http://www.qinetiq.com

Model-based Operational Performance Assessment

1.3.4. Within Phase 2 and 3, **a second Work Area (WA2) specifically addressed the safety benefit aspects of STCA, with the aim of defining quantified performance requirements for STCA and STCA/TCAS interoperability**. As illustrated in Figure 2, this work area consisted in the modelling of current STCA and TCAS operations in Europe, the evaluation of STCA performance (including the level of interaction with TCAS) in realistic operational scenarios and sensitivity analysis of factors influencing this performance.

1.3.5. The cornerstone of this evaluation is the use of the encounter model-based methodology commonly used in ACAS safety studies such as ACASA or ASARP ([ACASA], [ASARP]). A series of models have thus been developed, which constitutes a realistic framework in which STCA performances can be investigated. These models include a model of conflicts in which STCA or TCAS might be involved, a model of the EUROCONTROL Reference STCA System, a model of radar ATC surveillance means and specific models of controller and pilot behaviour in safety-net related occurrences.

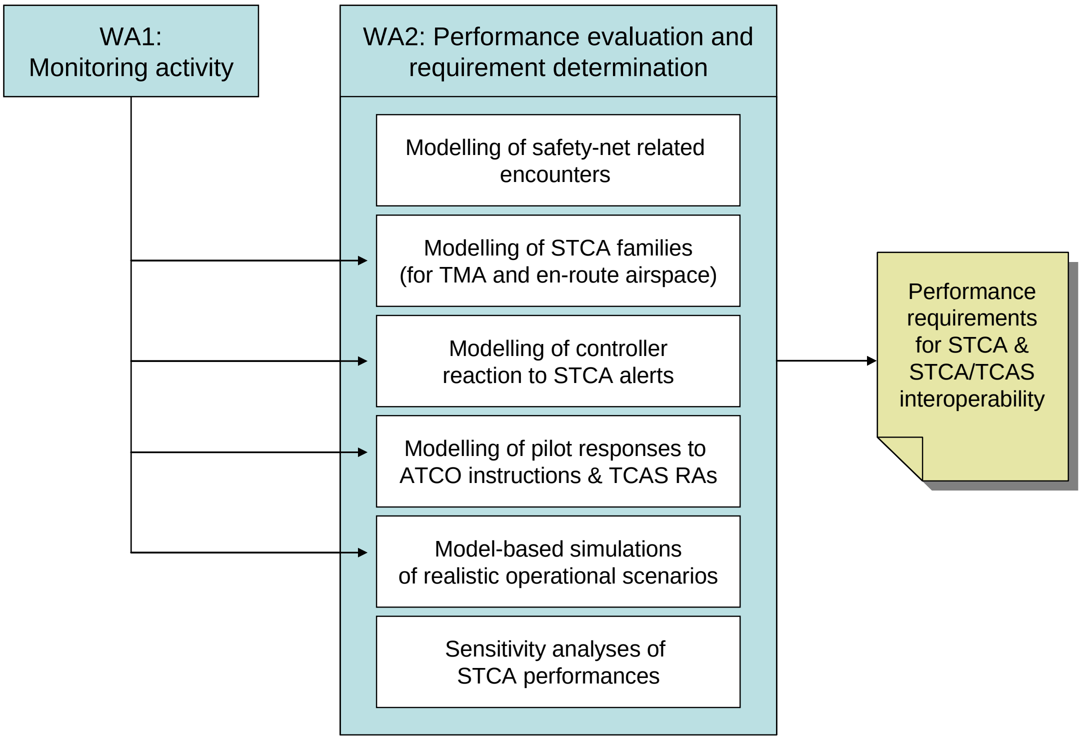


Figure 2: Modelling and Performance Requirement Determination (Work Area 2)

1.3.6. Based on the WA1 monitoring outcomes, a number of scenarios have been defined (and investigated in model-based simulations) that covers a wide range of realistic STCA environment, implementations and operations as observed in Europe. In addition, sensitivity analyses have been set up to help identifying the main factors influencing the likelihood of STCA alerts, their operational relevance, their potential efficacy and the level of interaction between STCA and TCAS.

Real-time experimentation

1.3.7. An optional third Work Area (WA3) was initially planned to be conducted within Phase 2 and 3, which consisted in a real-time experiment with controllers and pilots in-the-loop to complement the findings of WA1 and to help defining operational requirements supporting an overall operational concept for joint STCA / TCAS operations. This optional work was not launched due to lack of funding.

Operational Safety Assessment

1.3.8. Within Phase 2 and 3, **a fourth Work Area (WA4) specifically addressed the safety assurance aspects of joint STCA and TCAS operations, in the prospect of defining quantified safety requirements for STCA**. Building upon the WA1 monitoring outcomes, both qualitative and quantitative safety hazard analyses have been performed with a specific focus on the identification and assessment of operational factors, in addition to the environmental and technical factors, that may influence the safety of joint STCA and TCAS operations.

1.3.9. As illustrated in Figure 3, the safety assessment first consisted of STCA-related operational hazards identification and risk assessment, including an assessment of their operational effects, mitigation and severity, and an apportionment of ATM safety targets to derive safety objectives. In a second step, it focused on the determination of the (human and system) failure modes possibly leading to the identified operational hazards. Following a top-down apportionment of the safety objectives determined in the first step, safety requirements were eventually derived for STCA.

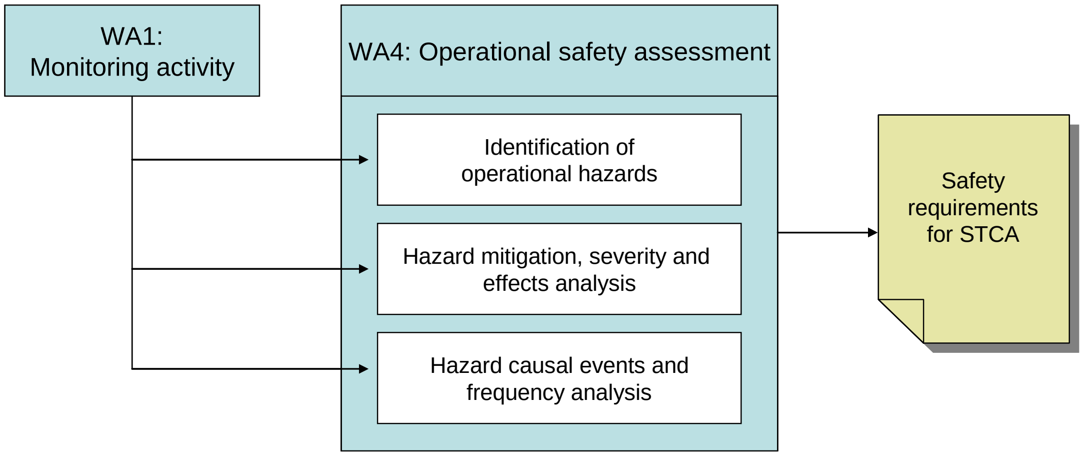


Figure 3: Operational Safety Assessment (Work Area 4)

Synthesis and Guidelines

1.3.10. To complete Phase 3, **a fifth Work Area (WA5) aimed at consolidating the main project outcomes and summarising all the work performed during the three project phases**. The consolidation work included the development of candidate operational, safety and performance requirements for STCA and STCA/TCAS interoperability using a process similar to the EUROCAE ED78A and RTCA DO-264 guidelines ([ED78A]). The opportunity was also taken to draw conclusions on how the complementary 'success case based' and 'failure case based' approaches to safety assessment as recommended by the EUROCONTROL Safety Assessment Made Easier ([SAME]) have been implemented in the present study.

1.3.11. The project was brought to an end with the present final report. As illustrated below, this report builds upon other key deliverables of the PASS project, including the (WA1) monitoring reports (see [D64], [D79], [D96] and [W38]), the (WA2) model-based performance evaluation reports (i.e. Phase 2 Interim report [D137] and Phase 3 Final report [D170] and the (WA4) operational safety assessment reports (i.e. Phase 2 Interim report [D130] and Phase 3 Final report [D162]).

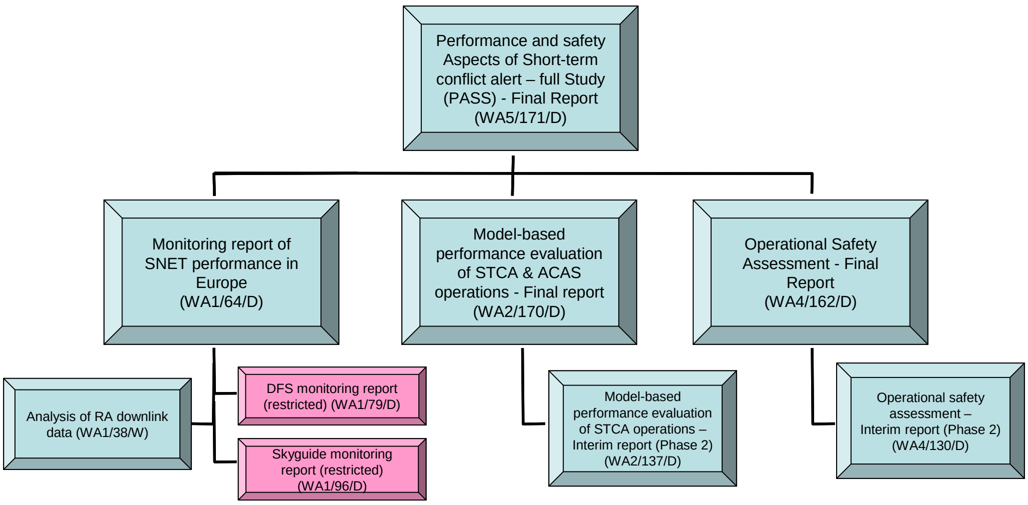


Figure 4: Main Project Deliverables

1.4. *Document overview*

1.4.1. Following this introduction of the project and the context in which it has been conducted, Section 2 provides background material on collision avoidance systems, both airborne and on the ground.

1.4.2. Section 3 describes the operational monitoring of STCA and TCAS related occurrences, which was conducted in the early phases of the project, and the different ANSP approaches with regard to STCA operation that became apparent through this monitoring.

1.4.3. Section 4 presents the STCA and TCAS performance assessment that has been conducted using the model-based methodology, as well as the resulting candidate performance requirements.

1.4.4. Section 5 presents the operational safety assessment of joint STCA and TCAS operation, as well as the candidate safety requirements resulting from this assessment.

1.4.5. Lastly, Section 6 summarizes the main achievements and findings of the PASS project, and proposes elements to be considered for future work and recommendations.

1.4.6. It has to be noted that the present report does not contain all the results obtained during the monitoring and the safety and performance assessments, but some are used for illustrative purpose throughout sections 3 to 5. Readers interested in more detailed results from any of these areas should refer to the appropriate deliverables, which are referenced in section 7.3.

2. Background on collision avoidance systems

2.1. General

2.1.1. ICAO [ATM-OCD] has defined three layers for conflict management: "*Strategic Conflict Management, Separation Provision and Collision Avoidance*". Being a ground-based safety net against mid-air collision, STCA is part of the third layer like the airborne safety-net ACAS.

2.2. Role of SCTA

2.2.1. EUROCONTROL's Specification [ES11] defines STCA as: "*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.*"

2.2.2. It also mentions that:

> STCA is a ground-based safety net; its sole purpose is to enhance safety and its presence is ignored when calculating sector capacity.
>
> STCA is designed, configured and used to make a significant positive contribution to the effectiveness of **separation provision and collision avoidance**.

2.2.3. The EUROCONTROL Safety Regulation Commission (SRC) policy ([EAM4-6]) also clarifies the specific role that ground based safety nets have within the ATM system with the three following basic principles:

- "Ground based safety nets by themselves should have the sole objective to contribute to safety".
- "Ground based safety nets should not be relied upon for separation assurance in the provision of Air Traffic Services."
- "The effect and contribution of ground based safety nets may be taken into account when an ANSP determines the achieved level of safety."

2.2.4. As a reminder, the ICAO Annex 11 - Air Traffic Services ([Annex11]) states that:

"*3.3.1 In order to provide air traffic control service, an air traffic control unit shall: […] C) issue clearances and information for the purpose of preventing collision between aircraft under its control and of expediting and maintaining an orderly flow of traffic*"

2.2.5. Although the sole goal of STCA is to prevent mid-air collisions, this goal may be achieved through different strategies with more or less overlap with, on one hand the separation provision function, and on the other hand the airborne collision avoidance function. This is illustrated on the representation of conflict management in Figure 5.

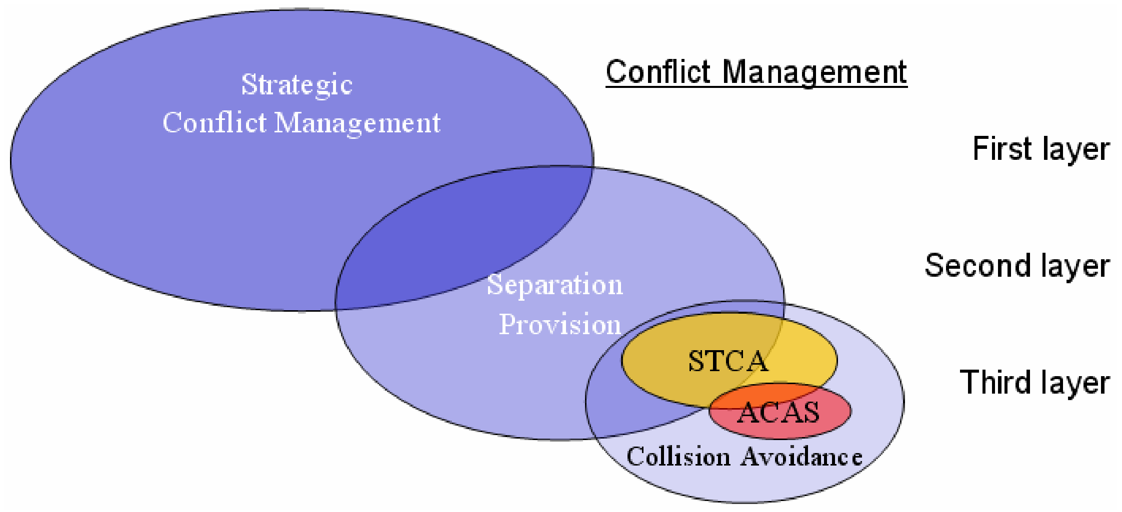


Figure 5: Position of STCA (and ACAS) within Conflict Management

2.2.6. 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.

2.2.7. Different operational concepts for the use of STCA and other local factors lead to different “separation thresholds” (and other parameters), as permitted by the general definitions of STCA and, as highlighted by the WA1 monitoring activity. This reality was taken into account by the WA2 modelling activities, where several configurations of the reference STCA model have been set up to mimic broad families of existing STCA systems and rule sets.

2.2.8. It must be noted that within the PASS study, the choice has been made to concentrate on scenarios where ATC is aiming at preventing collision by the issuance of clearances (or instructions) to at least one flight in order to maintain or restore separation (cf. requirements STCA-05, STCA-07 from [ES11]). The use of STCA to assist the controller in preventing collision through the provision of traffic or flight information was outside of the scope of the present study.

2.3. Role of ACAS

2.3.1. ICAO Annex 2 defines ACAS as "an aircraft system based on secondary surveillance radar (SSR) transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting[7] aircraft that are equipped with SSR transponders" (cf. ICAO Annex 2 – Rules of the Air). TCAS II version 7 is currently the only equipment complying with ACAS II standards.

2.3.2. The role of ACAS II is to mitigate the risk of mid-air collision. It serves as a last resort safety net irrespective of any separation standards. ACAS provides two levels of alert to the pilot, viz. Traffic Advisories (TAs) and vertical Resolution Advisories (RAs). A TA is a cue for the pilot to try to visually acquire the potential threat and to prepare for a possible RA. An RA is an indication to the pilot on how to modify or regulate his vertical speed so as to avoid a potential mid-air collision.

2.3.3. As stated in the ICAO Procedures for Air Navigation Services – Aircraft Operations (PANS-OPS) ([Doc8168]), in the event of an RA, pilots have to respond immediately by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane.

2.3.4. Naturally the safety benefits of ACAS II depend on the efficacy of the Collision Avoidance System (CAS) logic, but is also affected by the environment in which ACAS II is being operated, the way it is operated by the pilots, and the possible interaction between ACAS II and other lines of defence against the risk of mid-air collision, i.e. clearances and instructions issued by ATC in controlled airspace and the manoeuvres resulting from the application of the see-and-avoid principle.

2.3.5. Finally, it is worth noting that ACAS II is not designed, nor intended, to achieve any specific 'Target Level of Safety' (TLS). Instead, the safety benefit deriving from the deployment of ACAS II is expressed as a risk ratio, i.e. in terms of reduction in the risk of mid-air collision.

[7] In the context of ACAS, 'conflicting aircraft' is related to a risk of collision and not to the predicted violation of the separation minima applicable in the airspace by the ATC services.

3. Operational monitoring of STCA and TCAS related occurrences

3.1. General

3.1.1. Capturing current interactions between safety nets, as well as STCA performance and the determining factors influencing that performance, required the analysis of current ATC incidents where either STCA or TCAS was involved (safety-net related occurrences). Such an analysis was performed in several steps described hereafter, which eventually led to a better understanding of the typical sequence of elementary events in occurrences in which STCA and/or TCAS played a role and of the factors having a major influence on the features of this sequence (see [D64]).

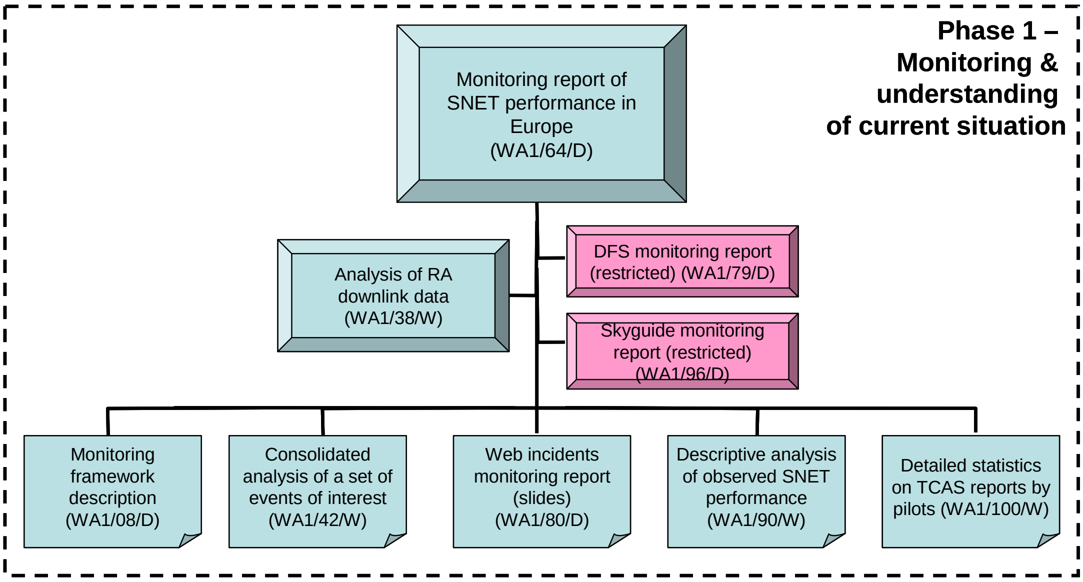


Figure 6: Main Deliverables (and Working Papers) of the Monitoring Activity

3.1.2. A monitoring framework ([D08]) was first developed, defining the kind of safety-net related occurrences that would be of interest, the participation asked from external partners, the inputs needed for each safety-net related occurrence, the data that would be extracted from these inputs and the metrics that would be computed for the whole set or some subsets of the safety-net related occurrences.

3.1.3. Safety-net related occurrences of interest were gathered from several States, with different STCA implementations. Three ANSPs participated in the gathering of operational data on occurrences of interest. As each ANSP did not have the same amount of resources to allocate to a monitoring effort in coordination with the PASS team, they had various levels of involvement:

- French ANSP **DSNA** contribution to PASS monitoring extended over seven months, from September 2007 to March 2008, and covered the Aix, Paris and Reims en-route control centres as well as Paris approach.

- Swiss ANSP **skyguide** contribution to PASS monitoring extended over three months, from May 2008 to July 2008, and covered the Geneva and Zurich control areas of responsibility ([D96]).
- German ANSP **DFS** contribution to PASS monitoring extended over one month, July 2008, and covered the Dusseldorf, Frankfurt and Munich control areas ([D79]).

3.1.4. Other safety-net related occurrences of interest were extracted from public sources from the following countries: the United Kingdom, Denmark, the Czech Republic, Ireland and Estonia ([D80]).

3.1.5. All occurrences with sufficient data (180) were analysed statistically to provide a descriptive view of the occurrences. The focus was on the description of the sequence of elementary events (STCA and TCAS alerts, pilot and controller actions and reactions, significant points) ([W90]). A complementary study highlighted the timing and quality of pilot TCAS reports ([W100]).

3.1.6. A more detailed analysis ([W42]) of a subset consisting of 12 occurrences focused on qualitative aspects in order to highlight the factors which most likely influenced the sequence of events in each occurrence, as well as the operational consequences of this sequence of events. In each detailed analysis of safety-net related event, the influencing factors were identified and described in detail.

3.1.7. Independently from the studies on safety-net related occurrences, a specific analysis of RA downlink data ([W38]) allowed the presentation of quantified results about the quality and reliability of RA downlink data. This analysis also provided a set of statistical figures dealing with the operational aspect in addition to the technical aspect and to make technical recommendations for the display of RA downlink on the controller working position.

3.2. Monitoring framework

Occurrences of interest

3.2.1. The monitoring activity looked for occurrences where at least one safety net was triggered. The interest of a given safety-net related occurrence was assessed by an operational expert within the PASS project team. Table 1 provides a summary of the safety-net related occurrences of interest.

3.2.2. All the safety-net related occurrences of interest were to be analysed quantitatively to obtain descriptive statistics on the occurrences and of the way in which they occur in general. However, this quantitative description may have failed to highlight a number of determining elements. There was a need to conduct more detailed analyses, but due to resource constraints this could not be done for all occurrences.

3.2.3. Therefore a subset of occurrences had to be selected, with the following criteria: it should represent a wide range of operational situations, sufficient information should be available for each occurrence, and each occurrence should be relevant in terms of human factors or other influencing factors.

STCA alerts only	Combined TCAS/STCA alerts	TCAS alerts only
No loss of separation as a result of ATCO intervention, before or after the alert	Late STCA in specific conflict geometries	Non-operative STCA
Loss of separation without TCAS RA	Lack of or late ATC avoiding instruction in response to STCA	TCAS threat non-eligible for STCA (*e.g.* military, VFR)
Non-operative TCAS	Conflicting avoiding instruction initiated by ATCO	Specific conflict geometries (*e.g.* 1,000 feet level-off, slow converging tracks)
	Lack of or late pilot response to ATC avoiding instruction	

Table 1: Summary of safety-net related occurrences of interest

3.2.4. Note that the safety-net related occurrences analysed during the monitoring activity were biased in favour of more serious incidents (due to the reported nature of the analysed occurrences). If readers wish to extrapolate the statistics presented hereafter (see section 3.3) to normal STCA performance, they should exercise both caution and expert judgment.

Data collection and analysis

3.2.5. As illustrated in Figure 7, collected data from the ANSPs included: radar data, RA downlink data and STCA data. Due to the diversity of the data sources, data processing was necessary to correlate the raw data collected for a given occurrence. The processed and correlated data were then analysed by operational experts. This resulted in 180 safety-net related occurrences of interest being selected and described, notably through a series of elementary events (i.e. safety net alert, human actor action, …), in a dedicated database.

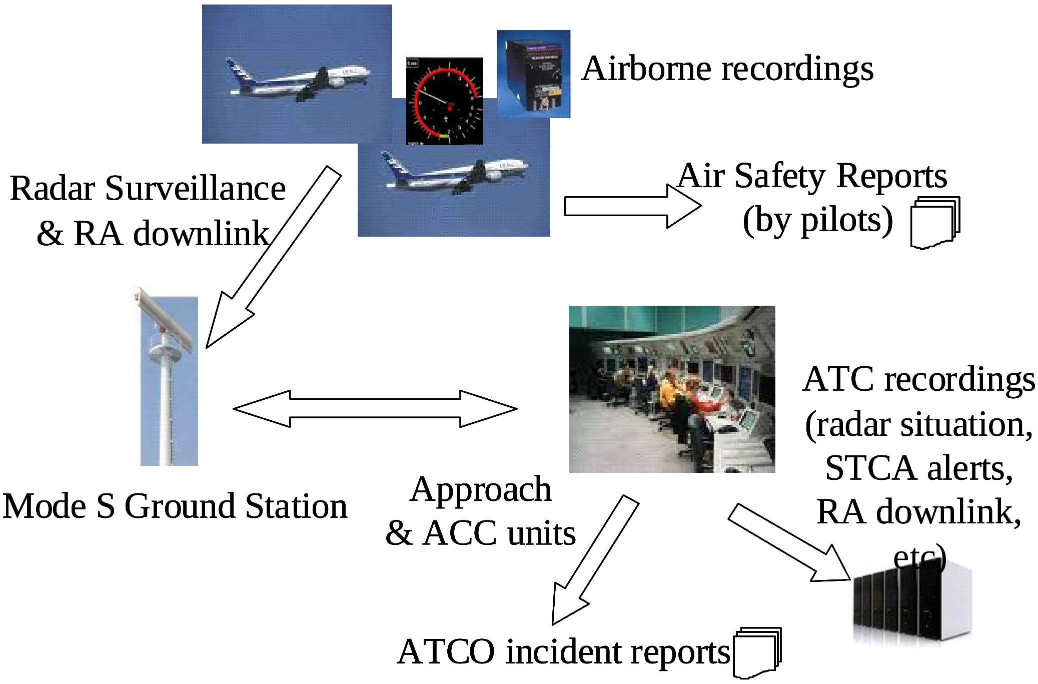


Figure 7: Sources of Monitoring Data

3.2.6. A descriptive statistical analysis used descriptive elements to provide a general picture of where (e.g. approach, en-route, flight phases, in between ATC units or sectors, etc.) and when safety-net related occurrences occur and how they develop (e.g. sequence of elementary events). A set of attributes and performance metrics characterising the safety-net related occurrences was computed on the set of 180 safety-net related occurrences.

3.2.7. For the 12 safety-net related occurrences with significant interest in terms of influencing factors, additional relevant information about the occurrence was requested: any existing incident report (Air Safety Report (ASR) by pilot, controller report, occurrence analysis report) and if possible the recording or transcription of the communications between ATC and the aircraft involved.

3.2.8. The qualitative analysis was based on the detailed analysis of 12 specific safety-net related occurrences to highlight the factors which most likely influenced the sequence of events in each occurrence, as well as the operational consequences of this sequence of events. In each detailed analysis of safety-net related event, the influencing factors were identified and described in detail.

3.3. Analysis of reported safety-net related occurrences in Europe

Adequacy of STCA alerts

3.3.1. The observed warning time of STCA alerts (i.e. the difference between the time of the STCA alert and the time at which separation is observed to be lost) is widely distributed and is measured to be 26 seconds on average in en-route airspace and 20 seconds in approach. It is largely influenced by the STCA parameters (en-route or approach, whether CFL is used, etc.), the conflict geometry and the optimisation strategy applied by the local ANSP.

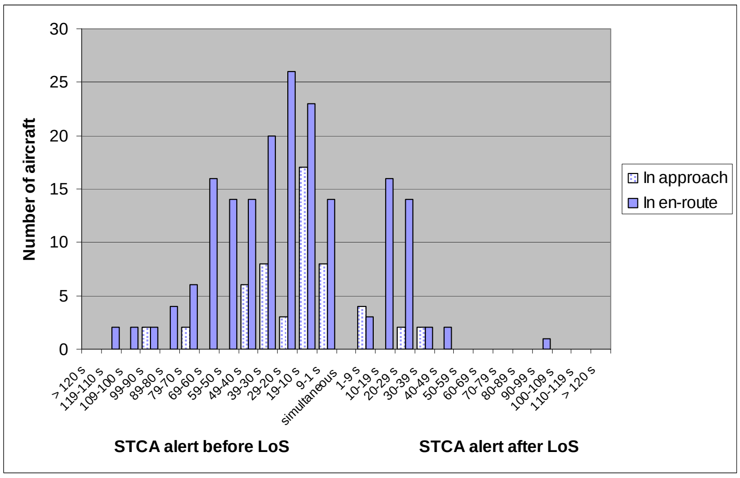


Figure 8: Distribution of time between STCA start and actual Loss of Separation (LoS)

Controller reactions to STCA

3.3.2. About one seventh (14%) of STCA alerts elicited no controller reaction. When the controller decides to issue an instruction, both aircraft are often acted upon, with an average 10-second time span between the instructions. The first instruction is issued around 10 seconds after the STCA alert on average, but a small proportion occurs before and another small proportion well after. The timing of the controller's reaction appears to be influenced by the STCA warning time and by his perception of the conflict. As an illustration, Figure 9 shows the difference between the time at which the STCA alert starts and the time at which the avoiding action is requested.

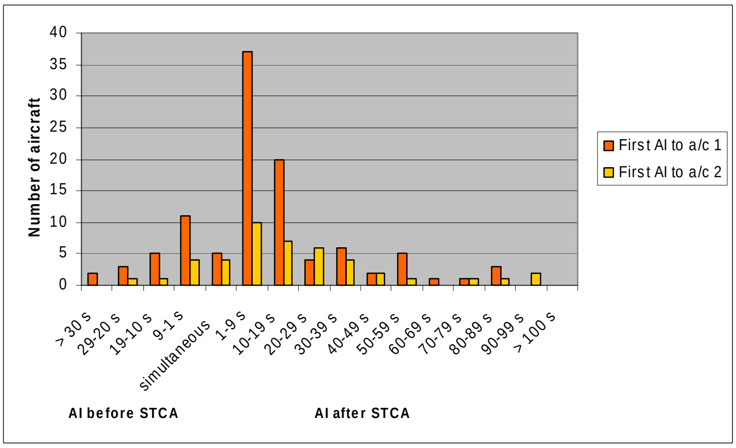


Figure 9: Distribution of time between first avoiding instruction (AI) and STCA start

3.3.3. Concerning controller instructions, the horizontal direction seems to be chosen predominantly in situations of high or medium horizontal convergence as well as for occurrences with aircraft at the same altitude. The vertical sense seems to predominate in standard 1,000-ft level-off situations.

Pilot reactions to controller avoiding instructions

3.3.4. Pilots respond to nearly all avoiding instructions, with a slight delay most of the time (around 10 seconds). The influence of the avoiding instruction phraseology is small (3 seconds). The timing appears to be influenced by the quality of the communications, previous provision of traffic information, successful visual acquisition and the compatibility of the instruction with the expected path and with an ongoing TCAS RA. As an illustration, Figure 10 shows the difference between the time at which the aircraft starts to manoeuvre and the time at which the first avoiding action is sent to this aircraft. It also distinguishes between avoiding actions using the urgency phraseology and those that do not.

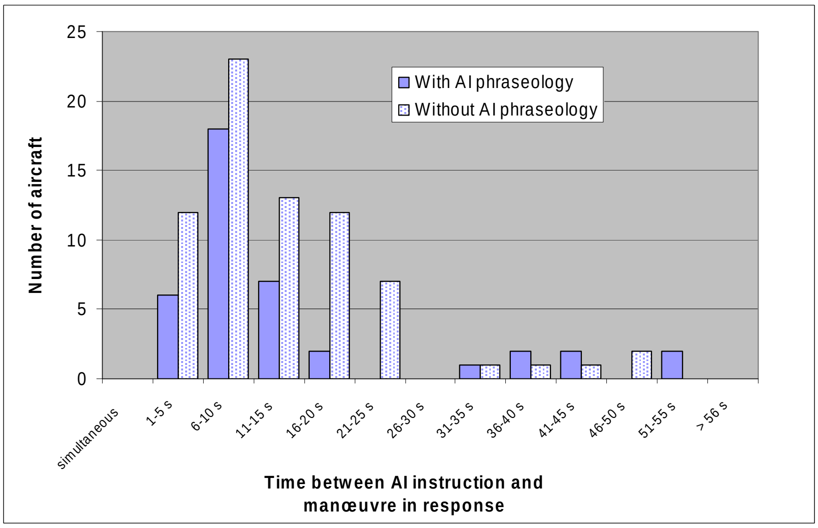


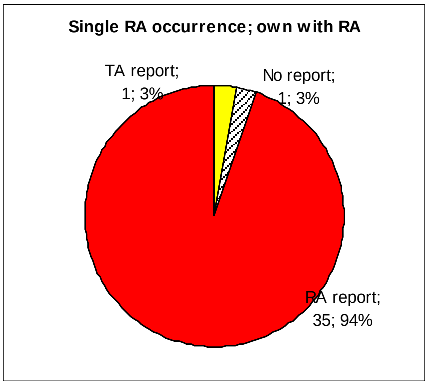
Figure 10: Distribution of time between first controller avoiding instruction and start of pilot's response

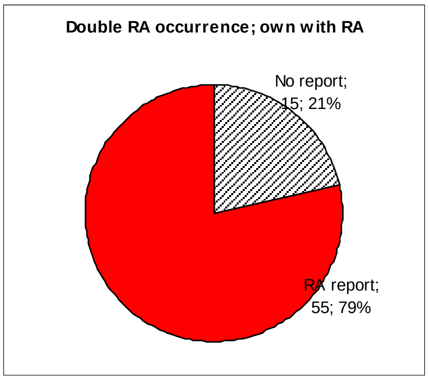
Pilot reactions to TCAS RAs

3.3.5. About one fifth (19%) of RAs in RA-only occurrences elicited no pilot reaction. Where there was a reaction, the average delay is compliant with TCAS logic assumptions (5 seconds). No significant difference was observed regarding compliance to RAs involving different directions. In 3 STCA / RA occurrences with an RA followed immediately by a controller vertical avoiding instruction, 2 featured a delayed reaction to the RA, maybe due to the use of avoiding instruction phraseology.

3.3.6. In occurrences where only one aircraft received an RA, most pilots (94%) reported a TCAS RA. In occurrences where both aircraft received an RA, A large majority of pilots (79%) reported their RA. This lower level illustrates the influence of a previous RA report within the same occurrence. Note that in both types of occurrences, the RA reporting rate is likely to be overestimated due to the focus on reported safety occurrences.

3.3.7. TCAS reports sometimes depart from standard phraseology. When standard phraseology is used, it might not be the applicable phraseology of the period (change in November 2007). Some RAs that do not require deviation are reported, although not required by ICAO provisions. Finally, TCAS reports do not always reflect the RA triggered onboard. As an illustration, Figure 11 shows the results of observed pilot reporting in occurrences where only one (left graph) or both (middle graph) aircraft received an RA, as well as what pilots effectively reported to ATC (right table).





Type of pilot report	Count
No report	16
TCAS alert (with no other detail)	5
TA	1
RA (with no other detail)	36
Climb	25
Descent	18
Adjust vertical speed	1
Maintaining current level	3
Clear of conflict	2
Total	107

Figure 11: Pilot reports during TCAS RA occurrences

3.4. *Analysis of recorded TCAS RA occurrences*

Technical analysis

3.4.1. Cross-checks between RA downlink data, Mode S track data and the results of TCAS simulations of aircraft trajectories, under the critical eye of an operational expert, made it possible to quantify not only those deficiencies which were already known in the downlinked messages but also a number of additional ones.

3.4.2. The most prominent deficiency was the overwhelming proportion (96%) of empty RA messages, a problem already known but still not resolved. Another example was incorrect threat-position information, which was downlinked in one third of the cases in which the threat aircraft was a Mode A/C aircraft. The cross-checking of "Communications and TCAS Capability" with the RA downlink data also highlighted errors such as incorrect format indicator (9%) and incorrect TCAS capability (17%).

3.4.3. Although none of the aforesaid deficiencies had any operational impact, their impact should be considered in the context of RA monitoring and display on a controller working position. On the other hand, more serious faults were detected in relation to "Flight Status". In six cases, faulty aircraft on the ground caused RAs to be triggered on board aircraft on final approach.

3.4.4. Despite these faults, the RA downlink technique using RA reporting worked properly in general, and no major issues were identified. Thanks to the radars used, the observed mean refresh rate was about five seconds, decreasing to three seconds for a quarter of the conflicts detected by several radars.

Operational analysis

3.4.5. Nearly 1,030 aircraft downlinked valid RA downlink messages. On average, RAs were triggered every 960 flight hours. However, taking into account only unintentional encounters, a civilian aircraft experienced an RA every 1,365 flight hours. Intentional encounters were civilian aircraft interceptions by fighters, military operations and also test flights with escorts

3.4.6. On average, the captured RAs lasted between 5 and 45 seconds (in 85% of cases), and some of them (5%) lasted more than one minute.

3.4.7. 880 conflicts were analysed. In each of them, there was at least one aircraft with an RA on board. Half of the conflicts were between two TCAS-equipped aircraft, but two thirds of these did not give rise to a coordinated RA. The main reason was the TCAS feature, designed to reduce the rate of RAs in 1,000-feet level-off geometries, which meant that no RA was issued on board the level aircraft. The second cause was an asymmetric view either of the horizontal or of the vertical situation on board each aircraft. A number of threat aircraft were operating TCAS manually in TA-only mode, but this was mainly the case for military aircraft.

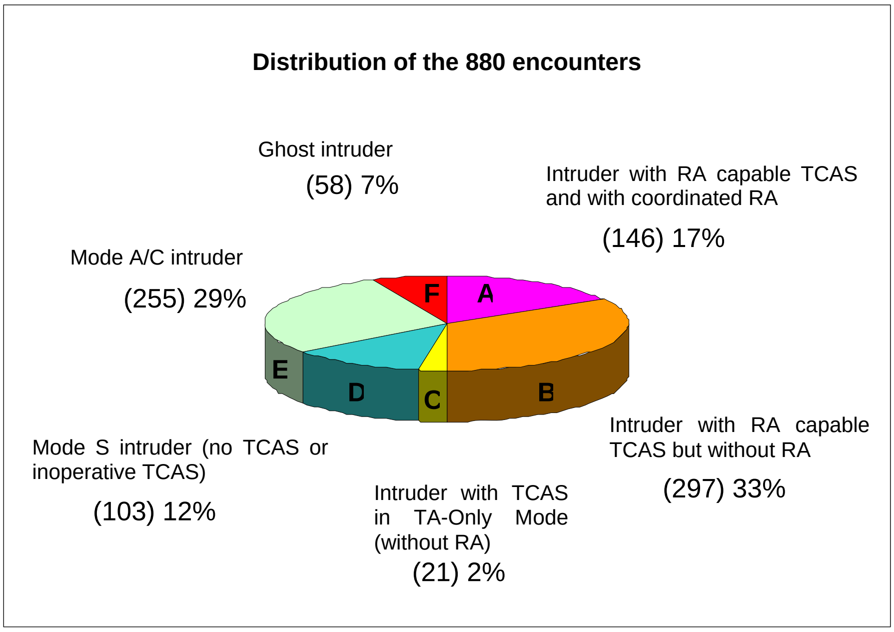


Figure 12: Intruder characteristics in valid recorded TCAS RA occurrences

3.4.8. About 12% of the threat aircraft were equipped with Mode S transponders only (without TCAS or with inoperative TCAS), and 29% were Mode A/C equipped. Of the Mode S threats, five were under TCAS mandate and suspected not to be TCAS equipped. One case of TCAS failure and another of TCAS switch-off were also detected.

3.4.9. About 70% of the conflicts were unintentional, 16% were classified as intentional and 14% could not be classified.

3.4.10. A non-negligible part (7%) of the conflicts corresponded to “ghost” threat aircraft. These were simulated threats during test flights, transponder tests on the ground with modified reported altitudes, false altitudes owing to garbling, originating mainly from a small number of military aircraft, and, lastly, self-tracking cases.

3.4.11. Among the unintentional encounters, the majority (61%) of RAs were solely “adjust vertical speed” RAs. In 24% of cases, the RA was a “climb” or “descend” RA, usually followed by a weakening RA to “adjust vertical speed”. About 10% were preventive RAs, occurring mainly between IFR arrivals and VFR flights.

3.5. Range of STCA system and rule sets in Europe

3.5.1. The study of safety-net operational occurrences spanning over several countries with different STCA implementations provided concrete examples of different operational concepts of STCA in Europe, especially when sectors from two different ANSPs were concerned. This was an opportunity to start thinking about a possible classification of STCA concepts and relate those to the ACAS concept

3.5.2. Based on the outputs from WA1 monitoring activities ([D64]) and the report on "European STCA environment" ([D31]), several approaches to the use of STCA have been identified and categorized, taking into consideration the differences of these approaches with the scope of ACAS. These categories first depend on the airspace in which STCA is operated. TMA airspace is characterized by lower applicable separation minima (3NM and 1,000ft) than en-route airspace (5NM and 1,000ft or 2,000ft minima), as well as difference in traffic speeds, which imposes different separation thresholds and warning time on STCA systems.

3.5.3. Similarly, each ANSP's strategy regarding the role of STCA guides the choice of these parameters' values towards more time-critical or less time-critical values and smaller or larger values for separation thresholds.

3.5.4. 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 13 below. The scope of ACAS is also indicated for comparison purpose, having in mind that both safety nets consider different hazardous situations (i.e. collision or LoS).

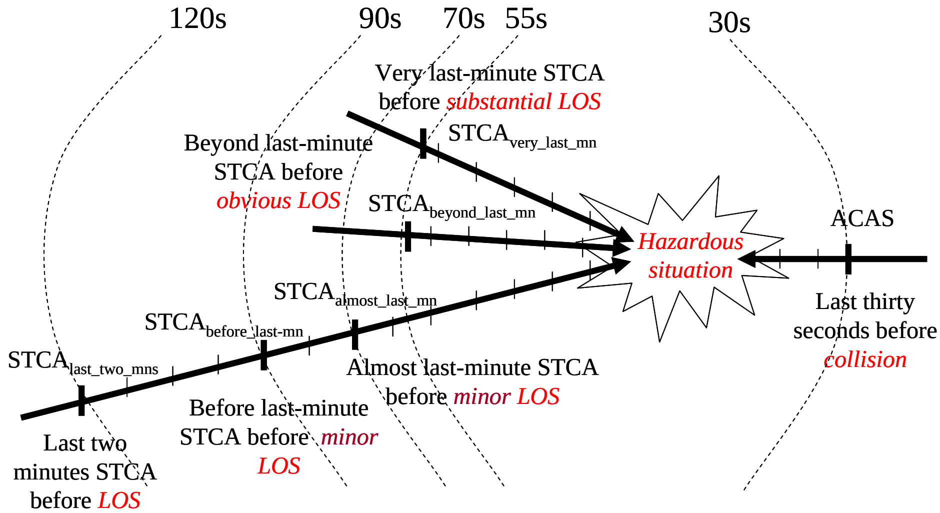


Figure 13: Families of STCA systems in en-route airspace

3.5.5. For TMA, the identified families of STCA appear to use only two sets of parameters for separation thresholds, but with each two different warning times. These families and the different approaches to the use of STCA in TMA are illustrated in Figure 14 below. The scope of ACAS is also indicated for comparison purpose, having in mind that both safety nets consider different hazardous situations (i.e. collision of LoS).

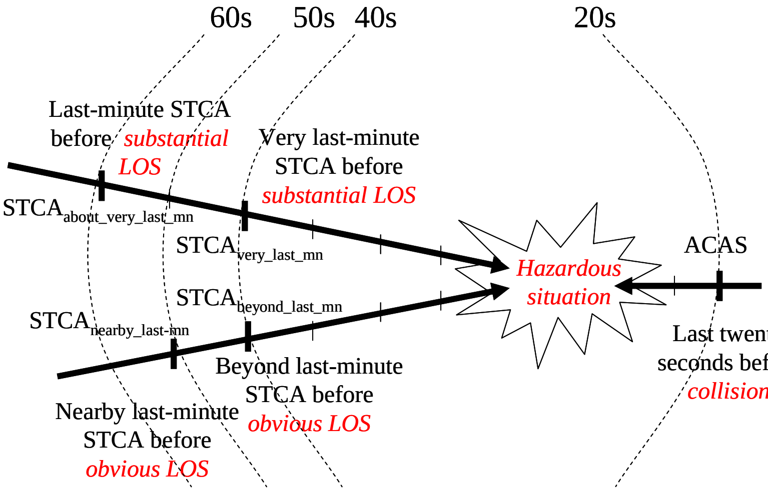


Figure 14: Families of STCA systems in TMA airspace

3.5.6. This classification scheme facilitated the modelling of STCA operations in the next step of PASS project (cf. Section 4) and was helpful in the establishment of requirements for STCA.

4. Model-based operational performance assessment of STCA and TCAS operations

4.1. General

4.1.1. As a precursor to the performance requirement determination for STCA, Work Area 2 developed a set of models that simulate STCA systems, their environment and operational use as observed during the WA1 monitoring activity. The development of these models was initiated during Phase 2 and completed during Phase 3 with the progressive introduction of improvements to increase the realism of the modelling.

4.1.2. These models include an encounter model generating operationally realistic situations in which STCA and TCAS might be involved ([D075]). This safety-net related encounter model captures the properties of relevant conflicts extracted from European radar recordings ([D071]). The behaviour of STCA systems in these conflicts is reproduced using an implementation of the EUROCONTROL Reference STCA System in an STCA model ([D116]). The CNS environment in which STCA is operated is also taken into account, notably with a model of ATC surveillance ([W36]). Lastly, the responses brought by human actors involved in STCA occurrences have also been implemented in specific controller and pilot models ([D115]).

4.1.3. Based on the WA1 monitoring outcomes and a complementary description of the European STCA environment ([D31]), a series of operationally realistic simulation scenarios have then been defined and investigated. This investigation started in Phase 2 with a set of basic scenarios in order to determine the parameters having the most significant impact on STCA performance. It was carried on in Phase 3 with the simulation of a wide range of realistic STCA implementations first assuming perfect CNS characteristics, as well as standard controller and pilot behaviour. It was finally completed by sensitivity analyses of the environmental and human factors possibly affecting STCA performance. These analyses were conducted using a set of operationally realistic scenarios specifically tailored for this purpose.

4.1.4. In parallel with the setting up of the model-based simulations, a set of metrics have been defined that allow quantifying the performance of STCA in any given scenario ([D120]). These metrics relate to the likelihood of STCA alerts, their operational relevance, their operational efficacy, and the compatibility with TCAS. Each of these STCA performance areas were thoroughly investigated during the model-based simulations carried out in Phase 3 of the project ([W161]).

4.1.5. In summary, Figure 15 shows the main deliverables and working papers developed within WA2 (during Phase 2 and Phase 3 of the project) and how each of them contributes to the model-based performance assessment of STCA and TCAS operations.

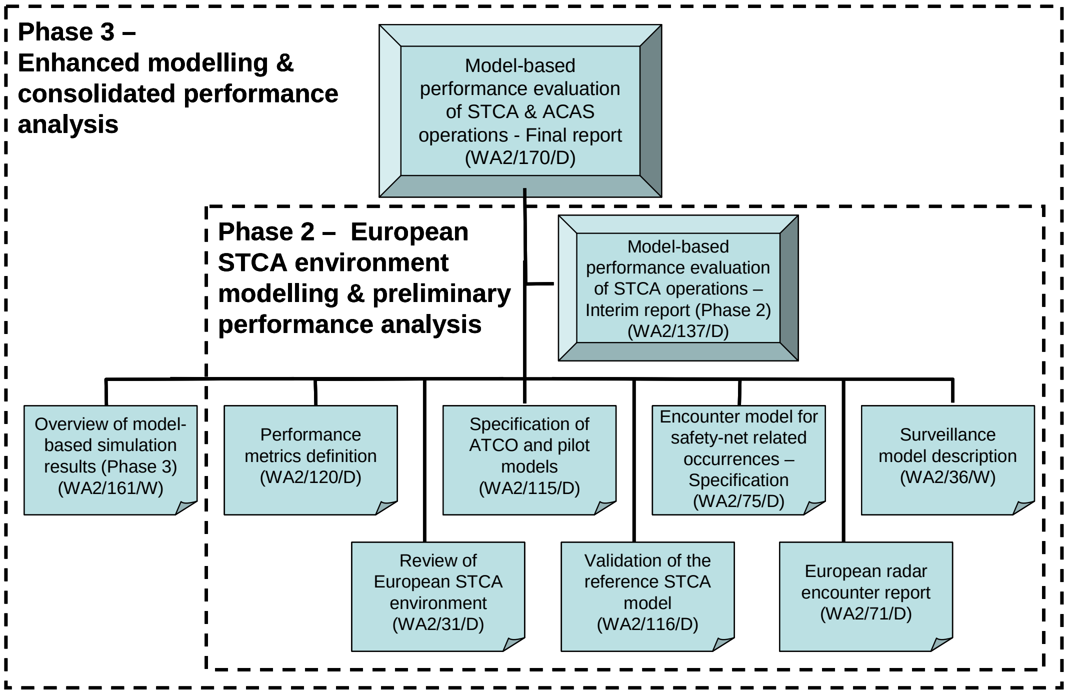


Figure 15: Main deliverables (and working papers) of the Model-based Operational Performance Assessment

4.2. Model-based performance evaluation framework

Underlying principles

4.2.1. The cornerstone of the STCA performance evaluation conducted within the present study was the extension of the encounter model-based methodology, already used in the ACAS field, to support the evaluation of the performance and safety benefits of STCA while taking into account the effect of TCAS operations.

4.2.2. The model-based methodology models both the system under assessment (i.e. STCA) and its environment (e.g. ATC surveillance, TCAS, controller, pilot). The performance of the system is quantified using a set of metrics measured on a model-based simulation implementing an operational scenario over a huge set of conflicts, corresponding to several years of traffic in Europe. Changing elements of the operational scenario simulated, whether on the system proper or in its environment, enables the investigation of the effects of key influencing factors on the overall system performance.

4.2.3. As illustrated in Figure 16, the work conducted within Work Area 2 of the PASS project has enabled the development of a set of models that constitutes a framework in which model-based simulations of STCA and TCAS operations can be conducted.

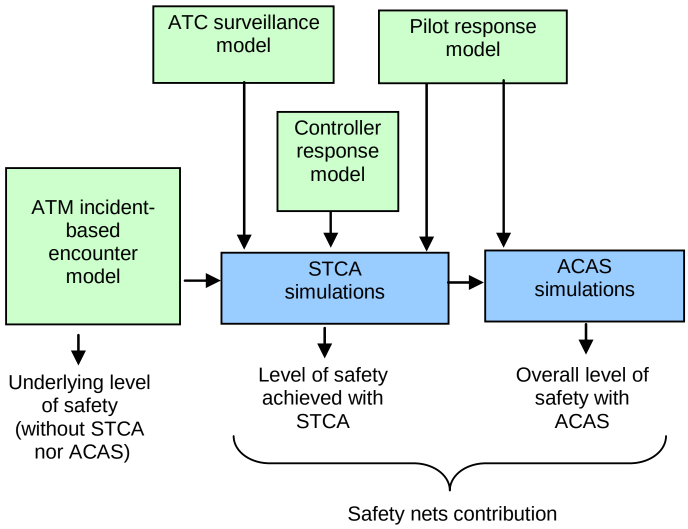


Figure 16: Framework for STCA performance evaluation

Key components of the framework

4.2.4. An essential component of this framework is an ATM incident-based encounter model designed to generate conflicts with a focus on losses of ATC separation in order to create situations with a potential for STCA alerts. This encounter model for safety-net related occurrences builds upon the European ATM encounter model delivered by the IAPA project. Its development was completed in Phase 3 of the PASS project with the progressive introduction of a set of improvements to increase the realism of the modelled conflicts (e.g. more operationally relevant altitude layers, new proportions of aircraft performance classes, refined altitude distribution within layers, more realistic distribution of aircraft turns and vertical rates, etc.). It is also able to focus on conflicts where both aircraft are eligible for STCA alerts (typically two IFR aircraft) or on conflicts where only one aircraft is eligible for STCA alerts (for e.g. an IFR and a VFR aircraft, an IFR and a military aircraft).

4.2.5. Another key component is the implementation of the EUROCONTROL Reference STCA System ([ES11]) in an STCA model that can be configured to suit different approaches towards the operation of STCA. This STCA modelling proved to be a powerful technique to evaluate and compare the performance of the various STCA families identified during the WA1 monitoring activity ([D064])

4.2.6. The other components of the simulation framework (i.e. the model of ATC surveillance and the models of controller's and pilot's responses following an STCA alert) also proved to be essential to investigate the influence of the CNS characteristics on the performance of STCA, as well as the influence of the human behaviour on the potential safety benefits that can be expected from STCA operation.

Performance evaluation areas

4.2.7. In the framework set in place, the comparative and sensitive analyses of STCA performances is supported by a set of metrics addressing four key performance areas as follows:

- the likelihood of STCA alerts (in terms of alerts per flight-hour);
- the operational relevance of STCA alerts, notably through the likelihood of “genuine” alerts, the trade-off between “missed”, “genuine” and “nuisance” alerts. From an operational perspective, the quality of the alerts (in terms of alert duration and continuity) is also of importance.
- the efficacy of “genuine” alerts, notably with respect to the time left for the controller to intervene, and achievable separation margins assuming realistic controller’s and pilot’s behaviour; and finally
- the level of STCA and TCAS interaction (in terms of combined alerts and relative timing) assuming both safety nets are being operated in the airspace.

4.2.8. Most metrics use the notion of conflict severity, which is an indication of the extent of the loss of ATC separation (when there is one) in a given conflict. Figure 17 illustrates the categories of severity which have been defined. Using this definition of severity, the effect of STCA, possibly combined with the effect of TCAS, can be qualified by comparing the “initial” severity of the conflict (without any safety net contribution) and the “final” severity (with the effect of the controller’s avoiding instruction prompted by STCA, possibly combined with the pilot’s response to any TCAS RA).

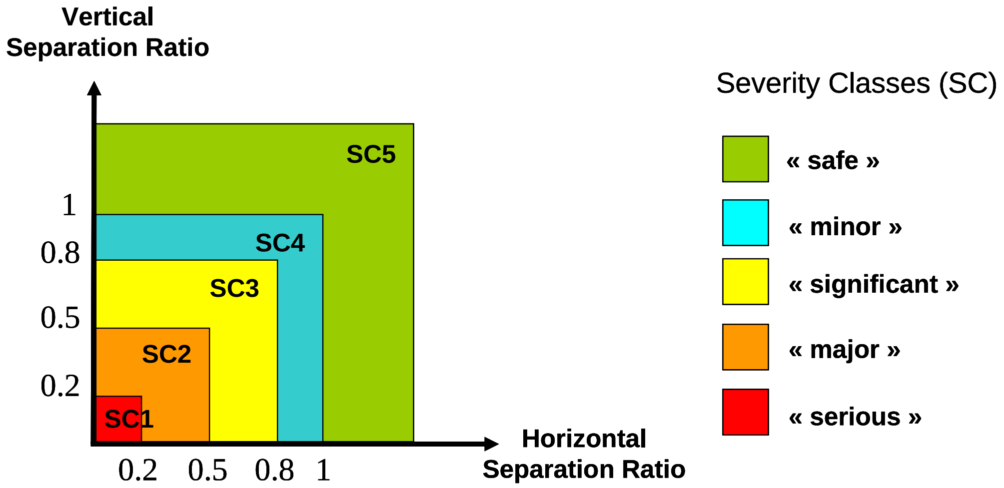


Figure 17: Definition of conflict severity classes

4.3. *Identified strategies for STCA implementation and optimisation*

4.3.1. The model-based simulations allowed characterizing in more depth the alternative strategies that ANSPs might follow when implementing and optimising their STCA system, which have been made apparent through the project monitoring. Three main strategies have thus been identified, based on both expert judgment and performance metric analysis using a best fit approach.

- A liberal strategy in favour of an STCA primarily designed to **make a significant contribution to the effectiveness of collision prevention (yet limited contribution to separation protection)** by alerting the controller of only potentially “major” separation infringements (i.e. less than half the separation minima applicable by ATC) and consequently quite effective in reducing the likelihood of alerts in case of conflicts with less “significant” separation infringements;
- An intermediate strategy in favour of an STCA primarily designed to **make a substantial contribution to the effectiveness of both separation protection and collision prevention** by alerting the controller of potentially significant separation infringements (i.e. less than four fifths of the separation minima applicable by ATC) with more or less unnecessary alerts in case of conflicts without separation infringement or with minor separation infringements;
- A conservative strategy in favour of an STCA primarily designed to **make an extensive contribution to the effectiveness of separation protection (and consequently to collision prevention)** by alerting the controller of any separation infringements with more or less unnecessary alerts in case of encounters without separation infringement.

4.3.2. The three strategies can be positioned on the representation of conflict management layers as in Figure 18.

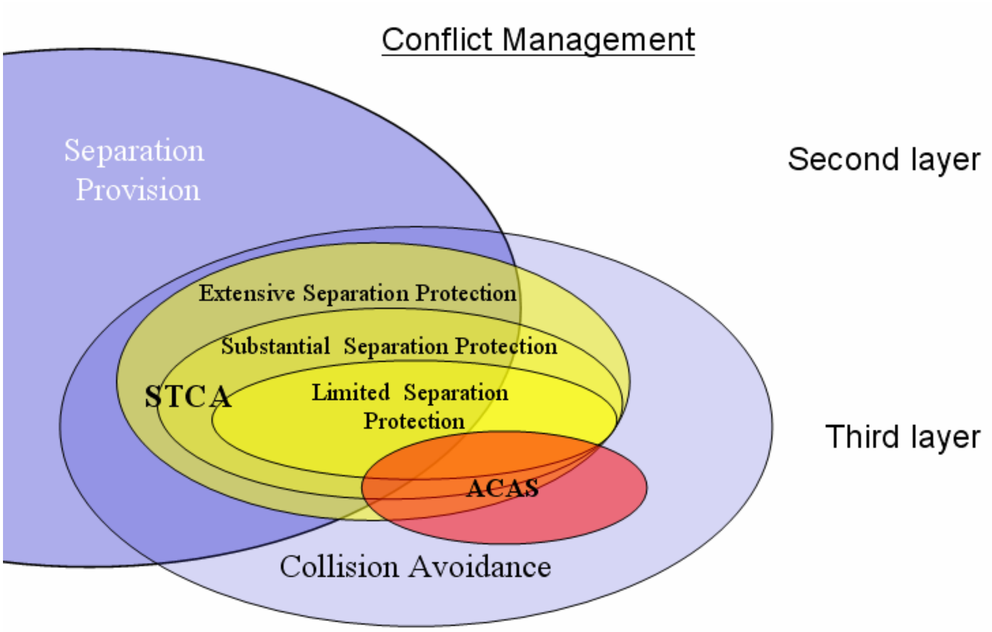


Figure 18: Position of the possible STCA strategies within Conflict Management

The strategy geared towards preventing mid-air collisions through limited separation protection has the most overlap with airborne collision avoidance while the strategy geared towards avoiding extensive ratio of separation infringements has the most overlap with the separation provision function.

4.3.3. The simulation results also highlighted that the notion of “genuine”, “missed” and “nuisance” alerts is likely to depend on the expectations of a given ANSP with respect to STCA, i.e. liberal, intermediate or conservative strategy for collision avoidance through respectively limited, substantial or extensive separation protection. This is illustrated in the table below, which outlines three possible definitions of “operationally relevant conflicts” (to be detected and alerted by STCA) based on the initial conflict severity (cf. 4.2.8).

4.3.4. The table below further defines the three possible classifications of STCA alerts (i.e. “genuine”, “missed” and “nuisance” alerts) that correspond to each of these strategies.

Liberal strategy for STCA implementation and optimisation	Intermediate strategy for STCA implementation and optimisation	Conservative strategy for STCA implementation and optimisation
Genuine alerts: alerts generated for “serious” and “major” conflicts (alerted SC1-SC2)	**Genuine alerts**: alerts generated for “serious”, “major” or “significant” conflicts (alerted SC1-SC3)	**Genuine alerts**: alerts generated for all conflicts (alerted SC1-SC4)
Missed alerts: alerts not generated for “serious” or “major” conflicts (un-alerted SC1-SC2)	**Missed alerts**: alerts not generated for “serious”, “major” or “significant” conflicts (un-alerted SC1-SC3)	**Missed alerts**: alerts not generated for any conflict (un-alerted SC1-SC4)
Nuisance alerts: alerts generated for “significant”, “minor” conflicts or “safe” encounters (alerted SC3-SC5)	**Nuisance alerts**: alerts generated for “minor” conflicts or “safe” encounters (alerted SC4-SC5)	**Nuisance alerts**: alerts generated for “safe” encounters (alerted SC5)

Table 2: Classification of STCA alerts based on initial conflict severity

4.3.5. Genuine alerts are expected to be generated with a sufficient warning time to allow the controller to achieve the result targeted by the ANSP. So the notion of “sufficient warning time” also depends on the ANSP chosen strategy for STCA implementation and optimisation. This idea is illustrated in the table below, which defines three possible definitions of “sufficient warning time” based on the conflict severity.

Liberal strategy for STCA implementation and optimisation	Intermediate strategy for STCA implementation and optimisation	Conservative strategy for STCA implementation and optimisation
Sufficient warning time: a warning time that would not result in a "serious" or "major" separation infringement assuming a prompt and appropriate controller reaction to the alert.	**Sufficient warning time**: a warning time that would not result in a "serious" or "major" or "significant" separation infringement assuming a prompt and appropriate controller reaction to the alert.	**Sufficient warning time**: a warning time that would not result in any separation infringement assuming a prompt and appropriate controller reaction to the alert.

Table 3: Definitions of sufficient STCA warning time based on initial conflict severity

4.4. Sensitivity analysis of factors influencing STCA performances

4.4.1. In order to assess and quantify the effects of the main influencing factors on STCA performance, three areas have been defined in which dedicated sensitivity studies have been conducted: STCA configuration and optional features, CNS environment of STCA and human behaviour ([D170]). It has to be noted that TCAS simulation has only been used when investigating STCA and TCAS interaction in the sensitivity analysis of STCA configuration and features. Each sensitivity analysis has been conducted on one or several selected STCA implementations, both in TMA and en-route airspace. The same approach was used for all analyses in order to allow for comparison between results: one or several options for the influencing factor under assessment were investigated in turn, while all other influencing factors were set to baseline values.

Influence of STCA families and configurations

4.4.2. For each of the families representing the range of STCA systems in Europe, three levels of implementation have been defined (basic, standard and extended implementations), corresponding to the use of more or less optional STCA features ([D031]). These optional features include the use of a target Flight Level[8] or uncertainties in the Linear Prediction Feature, the use of a Current Proximity Filter and the use of a Turning Prediction Filter. The model-based operational performance assessment computed the performance metrics defined in [D120] through fast-time simulation for all these combinations of STCA families and configurations ([D170]).

4.4.3. In this performance assessment of various STCA implementations, the other influencing factors were set to 'standard' values. Controller and pilot responses to STCA and/or TCAS alerts occurred after a fixed delay (while WA2 results showed they could vary significantly) and surveillance data were provided without gross errors (such as Mode C swaps or garbling, which the surveillance model is able to produce).

[8] This target Flight Level can either be the Cleared Flight Level or the Selected Flight Level.

4.4.4. The performance assessment demonstrated that all investigated STCA configurations show comparable alert rates for conflicts with a “serious” or “major” initial separation infringement. However, STCA corresponding to a liberal strategy result in a rate of alerts in less severe conflicts that is up to 100 times less than STCA corresponding to a intermediate or conservative strategy. The rate of nuisance alerts per flight hour is reduced by a factor of 3 to about 50 with the use of optional features, depending on the exact STCA implementation. The efficacy of STCA alerts is mostly linked to the warning time afforded by the STCA to the controller: with all STCA configurations, except those corresponding to a liberal strategy, the number of separation infringements was reduced by a factor of at least five compared to a situation with no STCA ([D170]). It has to be noted that in [D170], the warning time has been measured against the time when the ATC separation minima are lost, which *de facto* leads STCAs implementing a liberal strategy to be measured as providing shorter warning times than others.

4.4.5. As an illustration of the performance assessment process, Figure 19 provides the proportion of STCA alerts per initial severity of conflicts for the STCA families that have been considered in en-route airspace. This graph provides, for each level of initial conflict severity, the proportion of conflicts in which an STCA alert was issued for the five STCA families identified in en-route airspace. From this figure, the different strategies used by ANSPs with regard to STCA operation become apparent through the extent of a loss of separation for which an STCA alert is be issued. Based on this metric, it appears that the *very_last_mn* STCA family implements a liberal strategy, while the *before_last_mn* or *last_two_mns* families implement a conservative strategy.

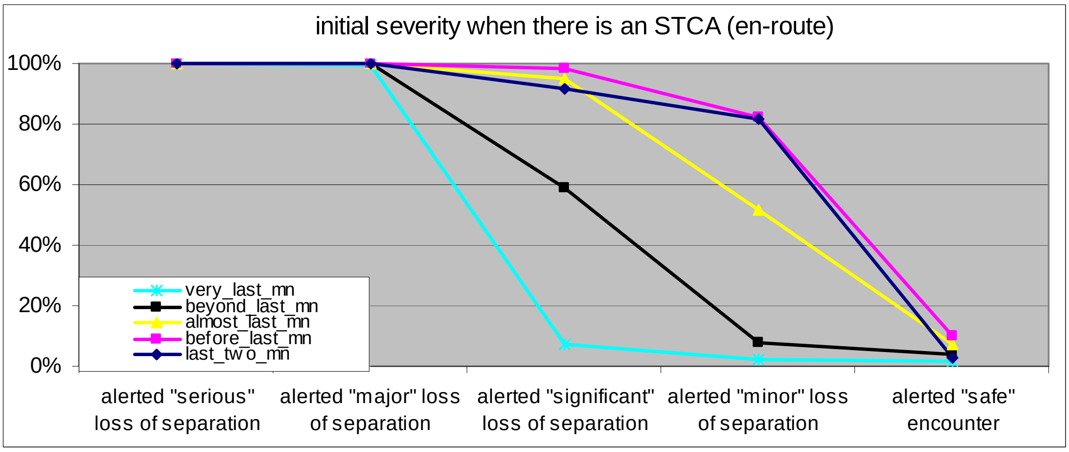


Figure 19: Illustration of STCA performance metric (STCA alert likelihood) computed through model-based simulation

4.4.6. To further illustrate the performance assessment, Figure 20 shows the cumulated number of conflicts in which both an STCA alert and a TCAS RAs have been issued. This metric has been computed on the same set of initial conflicts occurring in en-route airspace, when horizontal avoiding instructions are used by the controller model in response to STCA alerts. This figure illustrates how a short warning time, as used by STCAs corresponding to a liberal strategy, leads to an increased interaction between the two safety nets when horizontal avoiding instructions are given.

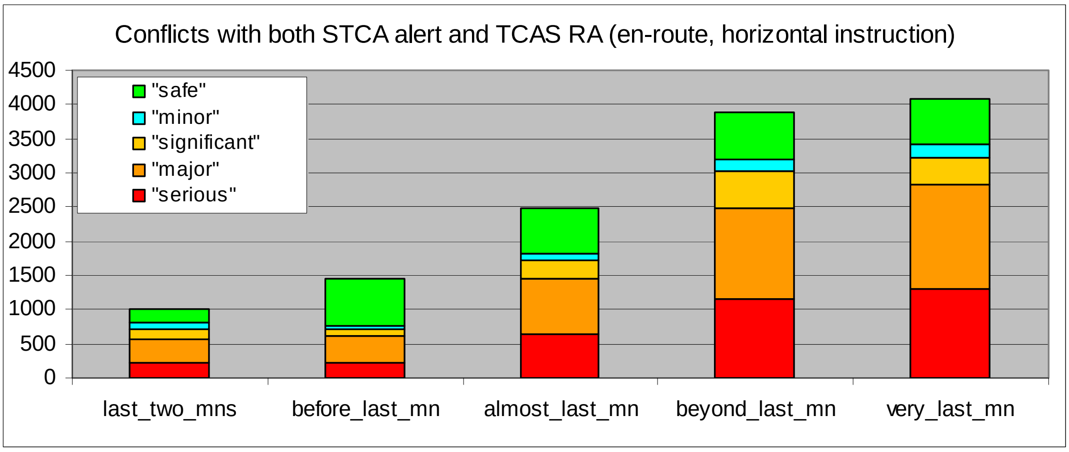


Figure 20: Illustration of STCA performance metric (STCA/ACAS interaction) computed through model-based simulation

Influence of CNS characteristics

4.4.7. The sensitivity analysis on the surveillance characteristics was carried out using four different surveillance scenarios for both TMA and en-route airspace. These scenarios, ranging from basic SSR environment to full Mode S coverage, varied the number of radars, their interrogation mode (i.e. Mode C or Mode S) and their rotation period. The quality of the surveillance data used by STCA was demonstrated to have an effect on the STCA alert rate, but not to the same extent as the STCA configuration. Improving the quality of the surveillance data was also showed to improve the quality of the alerts supplied by STCA to the controllers (i.e. by resulting in less split alerts) ([D170]).

4.4.8. Also as part of the CNS environment sensitivity analysis, an 'ideal' scenario in which all Mode S transponders report altitude in 25ft quanta has been evaluated for comparison purposes. It demonstrated that the transponder equipage scheme was shown to only have a marginal effect on the performance of STCA ([D170]).

Influence of human behaviour

4.4.9. Lastly, a sensitivity analysis on controller and pilot behaviour was carried out, addressing a broad range of realistic human performances in terms of delays, use of avoiding phraseology, etc. The performance analysis demonstrated that the more conservative STCA implementations are less sensitive to human performances, particularly when using vertical avoiding instructions which are typically more effective than horizontal avoiding instructions ([D170]).

4.5. Deriving quantified performance requirements on STCA

4.5.1. The results of the model-based performance evaluation weighted against the high-level operational requirements for STCA defined in [ES11] made possible the establishment of quantified performance requirements that should be met during nominal STCA operations.

4.5.2. These performance requirements are minimum values that the performance evaluation has demonstrated to be met by all configurations of STCA for the different families. Because the STCA performance assessment has been conducted over a generic airspace, rather than an actual one, they are proposed as candidate performance requirements against which the performance of operational STCA systems can be assessed.

4.5.3. In order to illustrate the performance requirement derivation process, Figure 21 shows how the model-based simulation results helped defining values for candidate performance requirements. The hatched zones correspond to a requirement on the acceptable minimum ratio of alerted separation infringements that was set using a performance metric related to the likelihood of STCA alerts. The proposed minimum ratios have been set so that all STCA families corresponding to a given strategy meet the requirement.

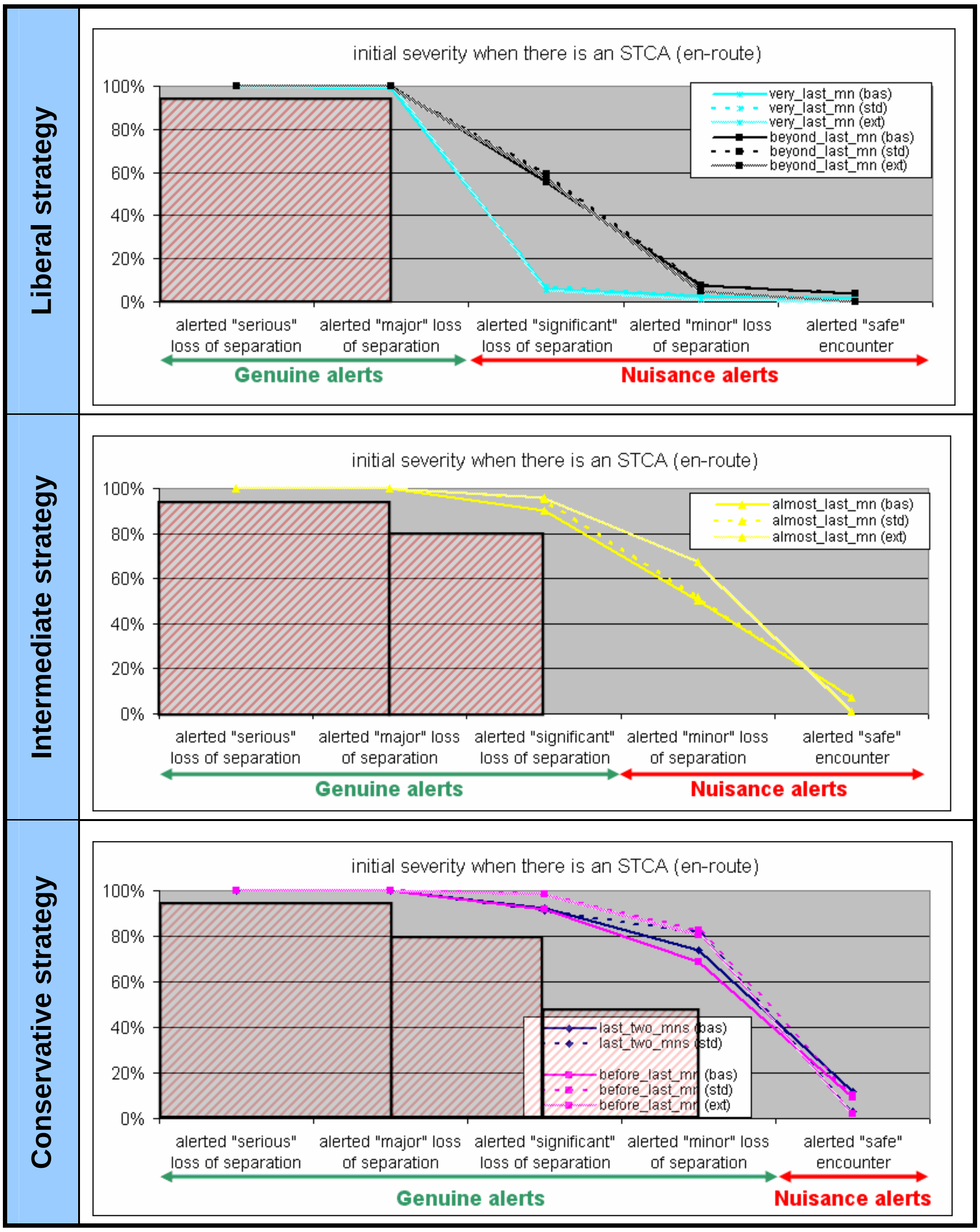


Figure 21: Illustration of performance requirement derivation

4.5.4. Table 4 provides the list of candidate performance requirements derived from the high-level operational requirements in ([ES11]). Additional details, including the rationale behind each performance requirement, can be found in Appendix A (see section B.4), while the whole requirement derivation process is detailed in [W168].

PR-#	**Performance Requirement (PR)**
PR-01 – Alerting capability of STCA depending on ANSP strategy	a) 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); b) When an 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); c) 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).
PR-02 – Acceptable minimum ratios of alerted separation infringements	a) When a liberal strategy is favoured, STCA ***shall*** produce alerts for at least 95% of initially "major", or worse, separation infringements; b) When an 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 initial "significant" separation infringements; c) 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.
PR-03 – Acceptable maximum proportion of nuisance alerts	a) 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 initially separation infringement; b) When an 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; c) When a conservative strategy is favoured, STCA ***shall*** produce alerts in less than 80% of situations with no initial separation infringement.
PR-04 – Acceptable maximum proportion of late alerts	a) When a liberal strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of situations with an initially "serious" separation infringement and 80% of situations with an initially "major" separation infringement, assuming a timely and appropriate controller's reaction; b) When an intermediate strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of situations with an initially "major", or worse, separation infringement and 80% of situations with an initially "significant" separation infringement, assuming a timely and appropriate controller's reaction; c) When a conservative strategy is favoured, STCA ***shall*** provide alerts that enable avoiding the hazardous situation in 95% of situations with an initially "major", or worse, separation infringement, 80% of situations with an initially "significant" separation infringement and 50% of situations with an initially "minor" separation infringement, assuming a timely and appropriate controller's reaction.

PR-#	**Performance Requirement (PR)**
PR-05 – Acceptable maximum ratio of short warning time alerts	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 an 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%.
PR-06 – Acceptable maximum ratio of short duration alerts	a) 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; b) When an 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; c) 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.

Table 4: Candidate Performance Requirements

5. Operational safety assessment of joint STCA and TCAS operations

5.1. General

5.1.1. A number of methodologies have been proposed as acceptable means of compliance with the provisions of ESARR 4 ([ESARR4]). Among these is EUROCONTROL's ANS Safety Assessment Methodology ([SAM]) which has been used in the present study. Using this methodology, the Operational Safety Assessment process derives Safety Requirements (SR) by considering unique Operational Hazards (OHs) introduced by STCA or existing OHs that an STCA system might adversely affect. These hazards are examined in order to control their likelihood and their effects.

5.1.2. In Phase 2 of the PASS project, preliminary hazard identification first pointed out the potential errors and malfunctions of the ATM system which are related to the functioning of STCA or to the interoperability of STCA and ACAS taken as an overall concept ([W91]). This qualitative analysis was based on the analysis of ATC incidents studied in WA1 of PASS, integrated with inputs from other studies (see Appendices B-3 and D-2 of [EGM20]). Having established this preliminary list of OHs, a quantitative event-tree analysis ([W102]) was performed to derive preliminary Safety Objectives based on the results of previous qualitative analysis as required by [ESARR4]. Safety Objectives limit the frequency of occurrence of hazards, such that the associated risk would be acceptable. This was followed by a summary and comparison of the qualitative and quantitative analyses ([D130]).

5.1.3. In Phase 3 of the project, the whole process was repeated to reach a consolidated list of OHs using expert judgment, analysis of other ACAS-related studies and a deeper understanding of cognitive aspects of the human actors' performance ([W151]). A consolidated event-tree analysis of these OHs was performed to derive refined Safety Objectives (D152]). Finally, a quantitative fault-tree analysis evaluated the possible (human and system) failure modes leading to these consolidated OHs and enabled the derivation of Safety Requirements on STCA ([W155]).

5.1.4. In summary, Figure 22 shows the main deliverables and working papers developed within WA4 (during Phase 2 and Phase 3 of the project) and how each of them contributes to the safety assessment of STCA and TCAS operations.

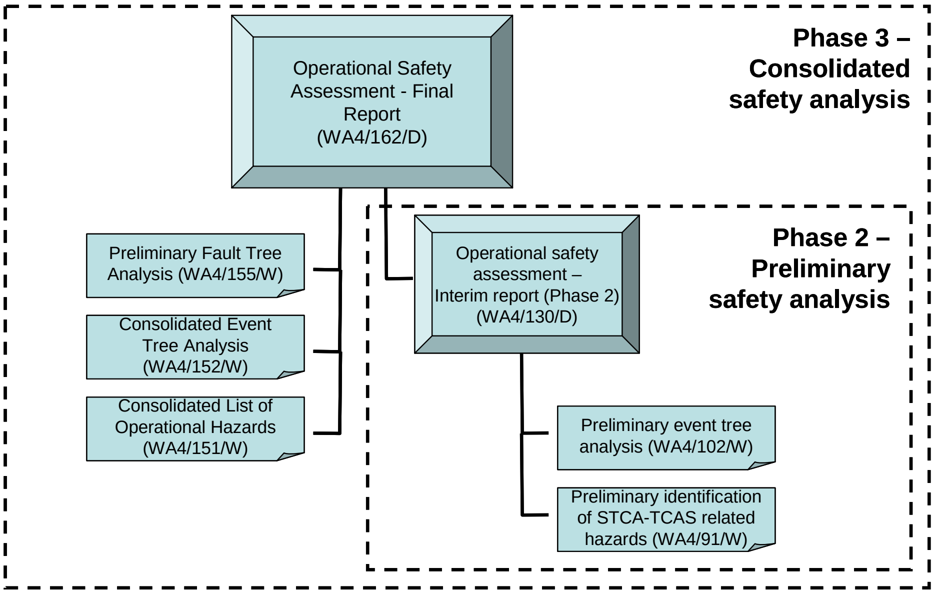


Figure 22: Main deliverables (and working papers) of the Operational Safety Assessment

5.2. *Event tree and fault tree Hazards Analysis*

5.2.1. The Operational Hazard Analysis (OHA) enabled the identification of a consolidated list of Operational Hazards (OHs) related to the operation of STCA and ACAS, considered as an overall concept. It has to be noted that these OHs already exist without STCA, but they are analysed in order to derive requirements on the STCA and assess the impact of STCA/TCAS interaction.

5.2.2. Each of these Operational Hazards was analyzed in detail in order to determine:

- The Basic Causes (BC), and their combinations, that can lead to the occurrence of the Operational Hazards;
- The Operational Effects (OE) that may result from the Operational Hazards;
- The Severity Class of each Operational Effect;
- The probability that the Operational Hazard generates that effect; and
- The Internal Mitigation Means, Environmental Conditions and External Mitigation Means that mitigate (or aggravate) hazards' effects.

5.2.3. The Basic Causes are determined during a Preliminary System Safety Assessment (PSSA), through the analysis of fault trees. The other elements are determined during a Functional Hazard Analysis (FHA) through the analysis of event trees. These different steps that constitute the Operational Safety Assessment are illustrated in Figure 23.

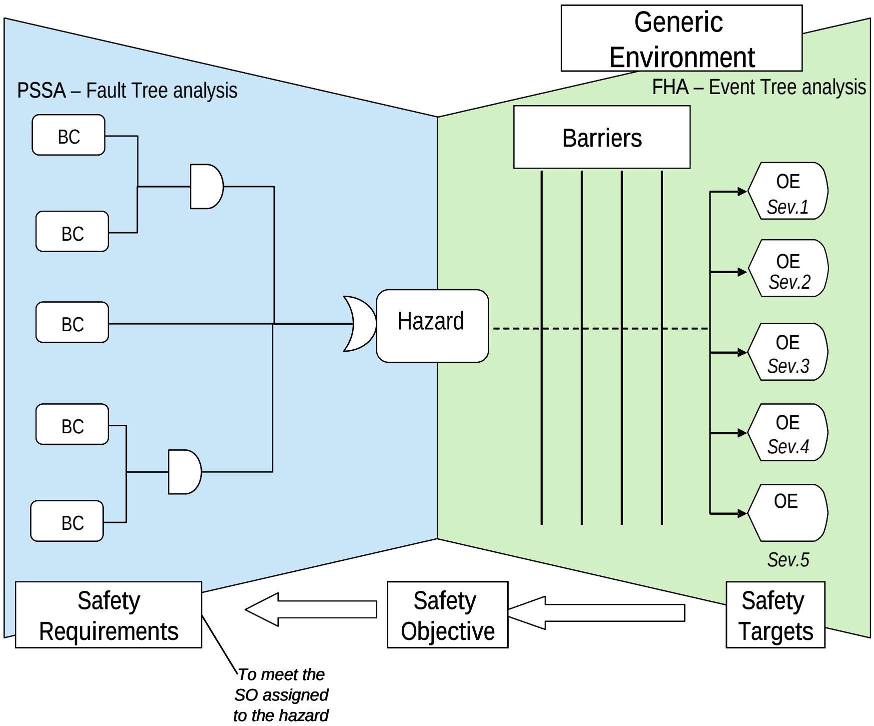


Figure 23: Operational Safety Assessment process

Operational hazard analysis

5.2.4. The analysis of an Operational Hazard begins assuming that it has occurred and modelling the Operational Effects of its occurrence by way of an Event Tree. These trees are typically built on a binary accounting for the “success” or “failure” of the mitigation means (i.e. procedural and environmental factors) in becoming effective. At the end of each branch, the effects of the hazards are assessed along with the corresponding Severity Class as per ([ESARR4]). The conditional probability of Operational Effects such as controller workload, pilot workload and collision, is then calculated based on the success/failure probability of each concerned barrier.

5.2.5. Table 5 provides the list of Operational Hazards resulting from the OHA, their assessed severity and probability of Operational Effect (Pe value). These OHs are defined at the boundary of the system under assessment, i.e. the controller(s) assisted by STCA to prevent collision between aircraft.

Operational Hazard	Severity	Pe Value
OH1: Lack of ATCO instruction to solve a short-term conflict	2	$6.0x10^{-2}$
OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA	3	$1.1x10^{-2}$
OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible	2	$6.9x10^{-2}$
OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible	2	$5.7x10^{-2}$
OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible	1	$1.3x10^{-4}$
OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible	1	$8.5x10^{-5}$

Table 5: Operational Hazards and Effects

Safety Objectives allocation

5.2.6. For the study purposes, ATM Safety Targets (corresponding to the maximum tolerable frequency of occurrence of effects directly caused by ATM for the severity classes 1 to 4 according to [ESARR4]) have been apportioned to the system under assessment and the retained Safety Targets are provided in the following table.

Severity Class	Safety Target [per flight hour]
1	$3.0x10^{-9}$
2	$3.0x10^{-6}$
3	$3.0x10^{-5}$
4	$3.0x10^{-3}$

Table 6: Apportionment of ATM Safety Targets to be considered

5.2.7. For each Operational Hazard, the Operational Effects probabilities (Pe values) determined during the OHA have then been used, together with the appropriate Safety Targets (ST), to derive a Safety Objective (SO) for each , i.e. the greatest frequency of the Operational Hazard such that the Safety Target is met for every Operational Effect, using the following formula:

5.2.8. $SO_i = \frac{ST_i}{Pe_i \times N_i}$, where i corresponds to each Severity Class (i from 1 to 4), Pe_i is the probability for the hazard to have a severity SC_i and N_i corresponds to the number of hazards having credible effects in that severity class i. It is assumed that the same number of hazards apply in En-Route and in TMA. Therefore, for each Severity Class, N_i is equal to 6 in both types of airspace.

5.2.9. These Safety Objectives were then retained as input to the subsequent Fault Tree Analysis. It is a simple way to directly ensure that if the most stringent safety objective is met for each Operational Hazard, then the other less stringent safety objectives of the remaining severity classes will be consequently met.

5.2.10. The table below provides the Safety Objective allocated to each of the identified OHs. These Safety Objectives are expressed per flight hour but for a better understanding they are also converted into Safety Objectives per year. Two examples are provided in the following table, as these Safety Objectives depend on the volume of traffic that a given ATSU handles in a year. ATSU-1 has a volume of 100,000 flight hours per year (corresponding to, e.g., an en-route ATSU in France) and ATSU-2 has a volume of 500,000 flight hours per year (corresponding to an ATSU equivalent to the size of MUAC).

Operational Hazard	**Safety Objective (per flight hour)**	**Safety Objective (per controlled hour) / ATSU -1** 100,000 flight hours per year	**Safety Objective (per controlled hour) / ATSU -2** 500,000 flight hours per year
OH1: Lack of ATCO instruction to solve a short-term conflict	8.3×10^{-6}	0.8 event every year	4 events every year
OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA	4.5×10^{-4}	45 events every year	225 events every year
OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible	7.2×10^{-6}	0.7 event every year	3.6 events every year
OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible	8.8×10^{-6}	0.9 event every year	4.4 events every year
OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible	3.8×10^{-6}	0.4 event every year	2 events every year
OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible	5.8×10^{-6}	0.6 event every year	3 events every year

Table 7: Safety Objectives allocated to Operational Hazards

Fault-tree hazard analysis

5.2.11. Following the Event Tree analysis and Safety Target allocation, a series of Fault Trees were created to permit the elaboration of Safety Requirements on the STCA system. These trees were constructed by decomposing the each Operational Hazard in to a combination of failures (a top-down approach is adopted) linked by different gates: "AND" gates (where all the input conditions must apply for the failure to occur) and "OR" gates (where any one of the input conditions is sufficient for the failure to occur).

5.2.12. In the fault trees, several kinds of basic events were combined to lead to the hazard. Those different kinds of basic events can be human failures to operate a basic task, external events to the STCA system or internal STCA failure. Quantitative values of the different causes of a given hazard were determined by combining two methods:

- A top-down allocation process: it consists in allocating the safety objectives towards the gates and finally the basic events composing the fault tree. This technique is usually applied for new systems; and
- A bottom-up allocation process: it consists in assigning a probability to each basic event based on engineering judgement.

5.2.13. Finally assumptions were made regarding external events, external failures and human errors, and Safety Requirements (SR) established so that each Safety Objective is met, concluding the safety hazard analysis.

5.3. Deriving quantified safety requirements on STCA

5.3.1. This last step permitted to apportion the Safety Objective to the different causes of a given Operational Hazard. Safety Requirements on basic causes common to several Operational Hazards were derived from the most stringent apportioned Safety Objectives that were applied through all fault trees, i.e. the most stringent frequency assigned to a basic cause was retained. Operational Hazards OH1 and OH5 are those that provided the most stringent values and thus led to the definition of the Safety Requirements.

5.3.2. It is important to note that all derived safety requirements in the Operational Safety Assessment (OSA) are generic and that they are based on conservative assumptions made on human errors, external event occurrences and on STCA configuration. To permit the elaboration of local safety requirements, which will correspond to specific ANSP needs, one possible approach would be to customise this safety assessment with local ANSP input data.

5.3.3. As a consequence the Safety Requirements derived from the OSA have to be considered as maximum values taking into account the assumptions used for the OSA, which can be relaxed in the case of actual STCA systems.

SR-no	**Safety Requirement (SR)**
SR-01	The likelihood of an error in implementation of STCA parameter region ***shall*** be less than **9.7x10^{-5} per flight hour**.
SR-02	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**.
SR-03	The likelihood of having STCA out of service ***shall*** be less than **2.1x10^{-4} per flight hour**.
SR-04	The likelihood of an excessive nuisance STCA alert rate ***shall*** be less than **1.2x10^{-3} per flight hour**.
SR-05	The likelihood of an excessive false STCA alert rate ***shall*** be less than **1.2x10^{-3} per flight hour**.
SR-06	The likelihood 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**.
SR-07	The likelihood of an erroneous design of STCA algorithm ***shall*** be less than **9.7x10^{-5} per flight hour.**
SR-08	The likelihood of a late STCA alert is issued due to erroneous parameters setting ***shall*** be less than **9.7x10^{-5} per flight hour**.
SR-09	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**.

Table 8: Candidate Safety Requirements

5.3.4. For an ANSP wanting to assess the safety of a local STCA system and check it against these candidate requirements, they would mostly need to be related to software development standards and validation level as the majority of the requirements pertain to a correct software implementation or parameter setting.

6. Conclusions and recommendations

6.1. Main achievements and findings

Project framework

6.1.1. The PASS project has studied performance and safety aspects of STCA operations, including technical, procedural and human performance issues, as well as considerations of the interactions with TCAS. The monitoring conducted within Phase 1 (October 2007-April 2009) enabled the development of an understanding of the current STCA environment in Europe, leading notably to the identification of different ANSP strategies with regard to the operation and optimisation of their STCA system. In addition, this monitoring provided a better understanding of the typical sequence of events during ATM occurrences in which STCA and/or TCAS played a role, and of the factors that have a major influence on this sequence.

6.1.2. Building on this foundation work, a modelling framework was developed during Phase 2 of the project (November 2008–December 2009) that enables the modelling of a reference STCA system conforming to the EUROCONTROL Specification ([ES11]), as well as the modelling of the various factors influencing its performance (i.e. typical conflicts in which STCA or TCAS might be involved, ATC surveillance means, and specific models of controller and pilot behaviour in safety net-related occurrences). The safety benefits aspects of STCA and TCAS operations were assessed by conducting model-based simulations using this framework and computing performance metrics pertaining to the likelihood, the relevance and the efficacy of STCA alerts, and to the level of interaction with TCAS.

6.1.3. An operational safety assessment of STCA and TCAS operations was also initiated during Phase 2 of the project that focused on the identification and assessment of operational factors, in addition to the environmental and technical factors, that may influence the safety of the joint operation of both safety nets. This safety assurance work was driven by the [ESARR4] requirements on risk assessment and mitigation in ATM and the explanatory material ([EAM4-6]) on ground-based safety nets.

6.1.4. The safety and performance investigation was completed during Phase 3 (January 2010–November 2010), which was concluded by the development of candidate operational, safety and performance requirements for STCA and STCA/TCAS compatibility. The work conducted within Phase 3 contributes to the definition of an overall concept of operations for STCA and ACAS.

6.1.5. An optional real-time experiment with both controllers and pilots in-the-loop was planned to complement the findings of Phase 1 and to help define operational requirements supporting an overall operational concept for joint STCA/TCAS operations. This optional work was however not launched due to lack of funding.

Project achievements and findings

6.1.6. Using the above framework, the project has been able to develop candidate safety and performance requirements using two different approaches for the safety and performance assessments. This work highlighted that the typical safety assessment methods show limitations when trying to provide a dynamic view of the issue (especially the safety benefits), and need to be complemented by the model-based assessment methodology that is more useful in that sense. The project has shown that the safety and performance assessment techniques used would also be appropriate for ANSPs wanting to assure the safe use of STCA and to assess the safety benefits brought by STCA before it is deployed. These techniques would usefully complement the monitoring of an STCA system in operation and aid the fine tuning of system parameters and thresholds.

6.1.7. The workshop on STCA & TCAS interaction and interoperability held on 27th and 28th March 2007 in Dübendorf raised a number of then unanswered questions which the PASS project has been able to, at least partially, answer. It notably appears that STCA cannot be "tuned" to prevent issuance of RAs, as all the STCA configurations investigated showed some degree of interaction with TCAS. The interaction with possible RAs can however be limited if controllers use procedures and working methods that are adapted to the ANSP's strategy with regard to STCA implementation and optimisation.

6.1.8. The work conducted within the project highlighted the need for ANSPs to choose and clearly define a strategy with regard to the implementation and optimisation of their STCA system. This strategy is key for the effectiveness of STCA in their airspace and for the setting up of appropriate performance targets, including those related to interaction with TCAS. The more conservative strategies (aiming at providing a substantial or extensive separation protection) were demonstrated to reduce the likelihood of undesired interaction between STCA and TCAS RA through the provision of generally longer warning times for the controller to intervene and prevent a TCAS RA from occurring. These strategies nevertheless proved less effective in keeping the number of nuisance alerts to an acceptable minimum, particularly when not using intent and trajectory information (from ATC tools or aircraft downlink data) to prevent unnecessary alerts during managed situations.

6.2. Future work

6.2.1. The work conducted within PASS with regard to safety assurance and safety benefits aspects of STCA operation should be reviewed in other arenas, such as EUROCONTROL Safety Regulation Commission for aspects related to Safety Net regulation and as the SJU SESAR Programme for aspects related to R&D.

6.2.2. The framework provided by the project to assess the safety assurance and benefits aspects of STCA operation can largely be re-used by other organisations.

6.2.3. In the context of an ANSP implementing an STCA system, the STCA and the environment used in PASS analyses are generic and the safety study would thus have to be instantiated with local data and inputs to conduct a safety assessment (for e.g. a safety case before deploying an STCA). Similarly, an organisation wanting to develop performance targets for its STCA system would have to qualify the performance assessment with local data and inputs.

6.2.4. In the context of SESAR, the PASS methodological framework should enable the investigation of the potential impact of new concepts, such as new separation modes, trajectory management or information sharing, on the effectiveness of STCA, as well as for the evaluation of potential changes to STCA.

6.2.5. As it stands, the modelling framework that has been defined and set up within the project is sufficient to study different options in the early stages of the STCA Lifecycle. The realism of this framework could nevertheless be improved in order to lead to performance requirements that more closely reflect the performance of actual STCA systems. Examples of such potential improvements are the combined use of horizontal and vertical manoeuvres by the controller response model, the introduction of non-nominal system or human behaviours in the fast-time simulations or an improved integration of STCA and TCAS simulation processes.

6.2.6. In order to progress on the definition of an overall operational concept of operations for compatible STCA and ACAS, some additional work would be required, such as controller and pilot in-the-loop simulations that would evaluate situational awareness, alert management and further determine the influencing factors. Within this context, the potential benefits of the use of TCAS RA downlink could also be investigated.

6.3. Recommendations

6.3.1. It is recommended that ANSPs conduct an operational monitoring of STCA and TCAS occurrences in their airspace in support to STCA performance analysis, including the level of interaction with TCAS.

6.3.2. It is recommended that the candidate operational, safety and performance requirements proposed by the project be promoted within the context of the SPIN Sub-Group and, possibly, that the EUROCONTROL STCA specification and guidance material be updated to include lessons learnt in this work.

6.3.3. It is recommended that the candidate requirements be further consolidated and developed up to pre-operational stage in the context of SESAR.

6.3.4. It is recommended that ANSPs implementing an STCA system take into account the project conclusions depending on the strategy they adopt with regard to the operation and optimisation of their system, especially those related to the STCA and TCAS interaction.

7. Bibliography

7.1. Reference documents

[ACAS] 'Surveillance Radar and Collision Avoidance Systems' – ICAO, Annex 10, Volume IV, 4th edition, July 2007

[Annex11] 'Air Traffic Services', ICAO Annex 11, Thirteenth edition, July 2001

[ATM-OCD] 'Global ATM Operational Concept', ICAO Doc 9854, First edition, 2005

[E-OCVM] 'European Operational Concept Validation Methodology', EUROCONTROL, Volume I, version 3.0, March 2010

[EAM4-6] 'Explanatory Material on Ground-Based Safety Nets', EUROCONTROL EAM4/GUI6, Edition 1.0, 15th April 2010

[EC552-2004] 'Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability regulation)'

[ED78A] 'Guidelines for approval of the provision and use of ATS supported by data communications', EUROCAE ED-78A, December 2000

[ESARR4] EUROCONTROL Safety Regulatory Requirement - ESARR4 Risk assessment and Mitigation in ATM (2001)

[ES11] 'EUROCONTROL's Specification for Short Term Conflict Alert', SPEC-122, Edition 1.1, 19th May 2009

[EGM20] 'EUROCONTROL Guidance Material for Short Term Conflict Alert, GUID-123, Edition 2.0, 19th May 2009
'Appendix A Reference STCA System'
'Appendix B-1 Initial Safety Argument for STCA System'
'Appendix B-2 Generic Safety Plan for STCA implementation';
'Appendix B-3 Outline Safety Case for STCA System'
'Appendix C Cost Framework for the Standardisation of STCA'
'Appendix D-1 Optimisation of STCA for ATCC Semmerzake'
'Appendix D-2 Functional Hazard Assessment of STCA for ATCC Semmerzake'

[MSAW09] 'EUROCONTROL's Specification for Minimum Safe Altitude Warning', Edition 0.9, 19th May 2009

[PANS-ATM] 'Procedures for Air Navigation Services - Air Traffic Management', ICAO Doc 4444 ATM/501, Fifteenth edition, November 2007

[PANS-OPS] 'Procedures for Air Navigation Services – Aircraft Operations', ICAO Doc 8168 OPS/611, Fifth edition, November 2007

[SAM] 'Air Navigation System Safety Assessment Methodology', EUROCONTROL, SAF.ET1.ST03.1000-MAN-01, Edition 2.1, 3rd October 2006

[SAME] 'Safety Assessment Made Easier – Part1 – Safety Principles and an Introduction to Safety Assessment', EUROCONTROL, Edition 1.0, 15th January 2010

7.2. Other external references

[ACASA] 'Final report on ACAS / RVSM Interaction in European Airspace', EUROCONTROL ACAS Programme, ACASA/WP3.6/185/D, September 2001

[ASARP] 'Final report on the safety of ACAS II in the European RVSM environment', EUROCONTROL Mode S & ACAS Programme, ASARP/WP9/72/D, May 2006

[FARADS] 'FARADS (Feasibility of ACAS RA Downlink Study) – Close-out Report', EUROCONTROL, 07/05/31-25, Edition 1.0, May 2007

[HFFAA] 'Human Factors Analysis of Safety Alerts In Air Traffic Control', Federal Aviation Administration, DOT/FAA/TC-07/22, November 2007

[IAMSAFE] 'I-AM-SAFE Feasibility Study Report', EUROCONTROL ATC Domain, I-AM-SAFE/WP5/15/D2, Version 1.1, March 2007

[IAPA] 'IAPA Project Final Report – Synthesis and guidelines', EUROCONTROL Mode S & ACAS Programme, IAPA/WP11/114/D, Version 1.2, October 2005

[OASIS] 'Open ATM System Integration Strategy', EUROCONTROL, 1992

[P481] 'Project Initiation Report: Evolution of Ground-Based Safety Nets', SESAR/04.08.01-PIR-Part I, Edition 00.01.01, April 2010

[P483] 'Project Initiation Report: Ground-Airborne Safety Nets Compatibility', SESAR/04.08.03-PIR-Part I, Edition 00.01.02, April 2010

[REQGL] 'Requirements and V&V Guidelines', SESAR JU, version 2.0

[SEMP] 'System Engineering Management Plan', SESAR JU, Version 2.0.1, February 2010

[WKS2007] Collision Avoidance: Quo Vadis?, STCA&ACAS Interaction and Interoperability Workshop Report, DETEC & EUROCONTROL, May 2007

7.3. Public reports and working papers

The following documents are available on EUROCONTROL website: http://www.eurocontrol.int/safety-nets/public/standard_page/PASS_deliverables.html

[D01] 'Project Management Plan', PASS/WA0/WP1/01/D, version 1.1, 28th January 2008

[D08] 'Monitoring framework description', PASS/WA1/WP1/08/D, version 1.1, 5th February 2008

[D31] 'Review of European STCA environment', PASS/WA2/WP1/31/D, version 1.2, 20th June 2008

[D64] 'Monitoring report of SNET performance in Europe', PASS/WA1/WP5/64/D, version 1.3, 28th April 2009

[D71] 'European radar encounter report', PASS/WA2/WP4/71/D, version 1.1, 20th May 2009

[D75] 'Encounter model for safety-net related occurrences – Specification', PASS/WA2/WP5/75/D, version 2.3, 9th May 2010

[D80] 'Web incidents monitoring report (slides)', PASS/WA1/WP6/80/D, version 1.0, 2nd December 2008

[D115] ‘Specification of ATCO and pilot models‘, PASS/WA2/WP6&7/115/D, version 2.0, 16th April 2010

[D116] ‘Validation of the reference STCA model’, PASS/WA2/WP2/116/D, version 1.0, 19th June 2009

[D120] ‘Performance metrics definition’, PASS/WA2/WP8/120/D, version 1.1, 2nd September 2009

[D130] ‘Operational safety assessment – Interim report’, PASS/WA4/WP5/130/D, version1.2, 23rd July 2010

[D137] ‘Model-based performance evaluation of STCA operations – Interim report (Phase 2)’, PASS/WA2/WP9/137/D, version 1.1, 5th February 2010

[D152] ‘Consolidated Event Tree Analysis’, PASS/WA4/WP4/152/D, version 1.0, 24th June 2010

[D162] ‘Operational Safety Assessment Final Report’, PASS/WA4/WP5/162/D, version 1.1, 10th September 2010

[D170] ‘Model-based performance evaluation of STCA and ACAS operations - Final report’, PASS/WA2/WP10/170/D, version 1.0, 10th September 2010

[W36] ‘Surveillance model description’, PASS/WA2/WP3/36/W, version 2.2, 26th April 2010

[W38] ‘Analysis of RA downlink data’, PASS/WA1/WP4/38/W version 1.5, 30th March 2009

[W42] ‘Consolidated analysis of a set of events of interest’, PASS/WA1/WP4/42/W, version 1.0, 31st January 2009

[W90] ‘Descriptive analysis of observed SNET performance’, PASS/WA1/WP5/90/W, version 1.0, 20th January 2009

[W91] ‘Preliminary identification of STCA-TCAS related hazards’, PASS/WA4/WP1/91/W, version 3.0, 17th April 2009

[W100] ‘Detailed statistics on TCAS reports by pilots’, PASS/WA1/WP5/100/W, version 1.0, 31st March 2009

[W102] ‘Preliminary event tree analysis’, PASS/WA4/WP3/102/W, version 1.1, 20th October 2009

[W151] ‘Consolidated List of Operational Hazards’, PASS/WA4/WP2/151/W, version 0.2, 1st April 2010

[W155] ‘Preliminary Fault Tree Analysis’, PASS/WA4/WP4/155/W, version 1.0, 20th August 2010

[W161] ‘Overview of model-based simulation results (Phase 3)’, PASS/WA2/WP10/161/W, version 1.0, 26th July 2010

[W163] ‘Guidelines for an overall concept of operations for independent compatible STCA and ACAS systems’, PASS/WA5/WP1/163/W, version 1.0, 26th August 2010

[W168] ‘Safety and Performance requirements’, PASS/WA5/WP2/168/W, version 1.1, 26th October 2010

7.4. Restricted reports

[D79] 'DFS monitoring report (restricted report)', PASS/WA1/WP6/79/D, version 1.3, 15th May 2009

[D96] 'Skyguide monitoring (restricted de-identified report)', PASS/WA1/WP6/96/D, version 1.1, 25th May 2009

Appendix A. Definitions, abbreviations and acronyms

The following definitions, abbreviations and acronyms have been used for the purpose of the project

A.1. Definition of terms

ACAS Airborne Collision Avoidance System – a system standardised in the ICAO SARPs that uses transponder replies from other aircraft to warn the pilot of a risk of impeding collision.

Hereafter, ACAS always refers to ACAS II – a system that generates traffic advisories (TAs) and also resolution advisories (RAs) in the vertical dimension, and whose carriage and operation is mandatory for many aircraft in Europe.

Alert Indication of an actual or potential hazardous situation that requires particular attention or action (Source EUROCONTROL's Specification of Short-Term Conflict Alert).

Hereafter, unless otherwise specified, the term “alert” refer to an STCA alert (and not to an ACAS alert).

ATC surveillance A means to detect and measure the position of aircraft in support of an ATC service (vectoring, monitoring and separation) in en-route and TMA airspace.

Barrier Barriers to hazards represented in the event trees are mitigation means that help in detecting and recovering from a hazard, once the hazard has occurred.

Conflict Convergence of aircraft in space and time which constitutes a predicted violation of a given set of separation minima.

Source: EUROCONTROL's Specification of Short-Term Conflict Alert (derived from ICAO Doc 9426)

Conflict is any situation involving an aircraft and hazard in which the applicable separation minima may be compromised.

Hazards that an aircraft will be separated from are: another aircraft, terrain, weather, wake turbulence, incompatible airspace activity and when the aircraft is on the ground, surface vehicles and other obstructions on apron and manoeuvring area.

Source: ICAO Doc. 9854 – Global Air Traffic Management Operational Concept

Encounter A traffic situation involving two (or more) aircraft in which STCA and/or TCAS may issue an alert.

Encounter (or conflict) severity An indication of the extent with which applicable ATC separation minima are infringed in a given traffic situation if a loss of separation occurred.

Distinction needs to be made between:

a) the initial severity of an encounter before any controller's avoiding instruction to maintain or restore separation;

b) the achieved encounter severity taking into account the effect of any controller's avoiding instruction to maintain or restore separation, possibly prompted by STCA; and

c) the final encounter severity taking into account the effect of all safety-nets (including that of TCAS).

Hereafter, unless otherwise specified, the severity of an encounter (or a conflict) refers to the initial severity, i.e. the severity that would exist in the absence of any controller's avoiding instruction to maintain or restore separation, possibly combined with the pilot's response to any TCAS RA.

Event tree An event tree is a graphical representation of the logic model that identifies and quantifies all possible outcomes following an initiating event, i.e. the hazard.

False alert Alert which does not correspond to a situation requiring particular attention or action (e.g. caused by split tracks and radar reflections).

Source: EUROCONTROL's Specification of Short-Term Conflict Alert

Genuine alert Alert which is correctly generated according to the rule set and is considered operationally appropriate.

Note: EUROCONTROL's Specification of Short-Term Conflict Alert requires STCA to detect and alert "operationally relevant conflicts", but no specific definition is given for such alerts

Ground-based safety net A ground-based safety net is a 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.

Source: EUROCONTROL's Specification of Short-Term Conflict Alert

Hazard Any condition, event, or circumstance which could induce an accident.

Source: ESARR 4

Note: In the qualitative analysis, hazard is more generically defined as a failure condition which could induce an incident or an accident. In the quantitative analysis a hazard is, in addition to the above definition, defined at the system boundary.

Missed alert Operationally relevant alert which is not generated.

Note: EUROCONTROL's Specification of Short-Term Conflict Alert requires STCA to detect and alert "operationally relevant conflicts", but no specific definition is given for alerts that are not generated during such conflicts

Nuisance alert Alert which is correctly generated according to the rule set but is considered operationally inappropriate.

Source: EUROCONTROL's Specification of Short-Term Conflict Alert

Operational requirement A statement of the operational features (e.g. policies, activities, functions, procedures, performances, etc) that enable the human actors to fulfil their tasks within the operational concept defined by an ANSP, and independent from any technical solution that could address the requirement.

Derived from EUROCAE ([ED78A] – 2000), OASIS ([OASIS] – 2002), EUROCONTROL ([E-OCVM] – 2010), and SESAR ([SEMP], [REQGL] – 2010)

Operationally relevant conflict Conflicts are operationally relevant when covered by the adopted rule set and optimisation strategy.

Source: EUROCONTROL's Specification of Short-Term Conflict Alert ([ES11])

Optimisation Strategy	Parameter optimisation strategy applied by an ANSP to optimise the performance of STCA in its airspace taking into account the relevant local factors. The objective of the parameter optimisation process is to allow alerting maximum operationally relevant conflicts with sufficient warning time while minimising nuisance alerts. Derived from EUROCONTROL's Specification of (and Guidance Material for) Short-Term Conflict Alert
Performance requirement	Set of requirements that define a function's performance, and expressed by a set of characteristics/attributes associated to all or part of a system. Source: EUROCAE Guidelines for approval of the provision and use of ATS supported by data communications ([ED78A]) Note: in the context of PASS, a function is to be understood as related to the service provided by a technical system.
Probability of effect	Probability that a hazard could generate a given effect. This probability can be obtained through event trees through the quantification of the failure/success of identified barriers.
RA	Resolution Advisory – a TCAS alert that indicates to a pilot how to adjust or regulate the vertical rate of the aircraft so as to avoid a mid-air collision
Rule set	Set of rules adopted by an ANSP when implementing STCA which determines the system features (including optional ones) and parameters that apply taking into account the relevant local factors. Derived from EUROCONTROL's Specification of (and Guidance Material for) Short-Term Conflict Alert
Safety objective	A safety objective is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur. Source: ESARR 4
Safety requirement	Safety requirements are risk mitigation means. A safety requirement is a requirement that when implemented, will help the system meet the safety objective. Safety requirements may take various forms, including organizational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics. Source: EUROCAE Guidelines for approval of the provision and use of ATS supported by data communications ([ED78A])
Separation	Spacing between aircraft, levels or tracks. Source: EUROCONTROL's Specification of Short-Term Conflict Alert ([ES11])
Separation minima	Horizontal and vertical separation minimum values applicable by ATC in a given environment. In radar controlled airspace, typical separation minima are: - 3 NM or 5 NM in the horizontal dimension; and - 1,000 feet (or 2,000 feet) in the vertical dimension.
Short duration alert	Alert that ends less than 20 seconds after having been generated. This definition is derived from an FAA Human Factor study ([HFFAA]), which suggested that "alerts lasting less than 20 seconds that do not result in operation errors can be considered nuisances because they deactivated before a response by the controller could have taken effect".
Split alert	Alert that is temporarily switched-off (at least once) during the alert time window.

STCA	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. Source: EUROCONTROL's Specification of Short-Term Conflict Alert
TCAS	Traffic alert and Collision Avoidance System – an aircraft equipment that is an implementation of an ACAS Hereafter, TCAS refers to TCAS II – the only equipment so far that is compliant with the ACAS II standards.
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.* *Note – In the context of the project, a hazardous situation is an operationally relevant conflict.* Source: EUROCONTROL's Specification of Short-Term Conflict Alert
Sufficient warning time	A warning time that enables avoiding a hazardous situation assuming a timely and appropriate controller's reaction to the alert.

A.2. Abbreviations and acronyms

ACAS	Airborne Collision Avoidance System
ACASA	ACAS Analysis (of EUROCONTROL)
AI	Avoiding Instruction
ANS	Air Navigation Service
ANSP	ANS Provider
ASR	Air Safety Report
ASARP	ACAS Safety Analysis – post-RVSM Project (of EUROCONTROL)
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
BC	Basic Cause
CFL	Cleared Flight Level
DETEC	Department of the Environment, Transport, Energy and Communication
DFS	Deutsche Flugsicherung
DSNA	Direction des Services de la Navigation Aérienne
EC	European Commission
E-OCVM	European Operational Concept Validation Methodology
ESARR	European SAfety Regulation Requirement (of EUROCONTROL)
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FARADS	Feasibility of ACAS RA Downlink Study (of EUROCONTROL)
FHA	Functional Hazard Analysis
FL	Flight Level
GAT	General Air Traffic
IAPA	Implications on ACAS Performances due to ASAS Implementation (project of EUROCONTROL)
I-AM-SAFE	IAPA – ASARP Methodology for Safety net Assessment – Feasibility Evaluation (of EUROCONTROL)
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
ILS	Instrument Landing System
LoS	Loss of Separation
NMAC	Near Mid-Air Collision
OASIS	Open ATM System Integration Strategy (of EUROCONTROL)
OAT	Operational Air Traffic
OE	Operational Effect

OH	Operational Hazard
OR	Operational Requirement
OSA	Operational Safety Assessment
PASS	Performance and safety Aspects of Short-term Conflict Alert – full Study (of EUROCONTROL)
PR	Performance Requirement
PSSA	Preliminary System Safety Assessment
RA	Resolution Advisory (in the context of ACAS)
RVSM	Reduced Vertical Separation Minima
SAM	Safety Assessment Methodology (of EUROCONTROL)
SARPs	Standards And Recommended Practices
SESAR	Single European Sky ATM Research
SJU	SESAR Joint Undertaking
SFL	Selected Flight Level
SC	Severity Class
SID	Standard Instrument Departure
SNET	Safety NET
SPIN	Safety nets Performance Improvement Network
SR	Safety Requirement
SRC	Safety Regulation Commission
SSR	Secondary Surveillance Radar
SSS	Surveillance, Separation & Safety
STAR	STandard ARrival
STCA	Short Term Conflict Alert
TA	Traffic Advisory (in the context of ACAS)
TCAS	Traffic alert and Collision Avoidance System
TMA	Terminal control Area
TLS	Target Level of Safety
VFR	Visual Flight Rules
WA	Work Area
WP	Work Package

Appendix B. Operational, Safety and Performance requirements for STCA

B.1. General

B.1.1. The high-level requirements that constitute the baseline for this study are extracted from EUROCONTROL's Specification for STCA ([ES11]) and the ICAO procedures ([PANS-OPS] and [PANS-ATM]). Only the requirements related to the operational use of STCA and TCAS have been retained.

<table>
<tr><th>REQ-no</th><th>Requirement title</th><th>Nature (scope)</th></tr>
<tr><td colspan="3">Requirement statement using the following writing convention in line with the convention stated in EUROCONTROL's Specification for STCA ([ES11]).
Requirements using the operative verb "<u>shall</u>" are mandatory to claim compliance with the Specification.
Requirements using the operative verb "<u>should</u>" are recommended.
Requirements using the operative verb "<u>may</u>" are optional.
Requirements using the operative verb "<u>will</u>" denote a statement of intent.</td></tr>
<tr><td colspan="3">Related high-level requirement(s):
For proposed new requirements derived from the PASS study outcomes, cross-reference to the related high-level operational requirement(s) in EUROCONTROL's Specification for STCA ([ES11]).</td></tr>
<tr><td colspan="3">Rationale (based on PASS outcomes):
For proposed amendments to existing requirement or for proposed new requirements, rationale with appropriate references to PASS study outcomes.</td></tr>
</table>

B.2. High-level operational requirements

B.2.1. The following baseline high-level requirements are extracted from EUROCONTROL's Specification for STCA ([ES11]).

STCA-01	Formal policy on the use of STCA	Organisational (ANSP)
The ANSP ***shall*** have a formal policy on the use of STCA consistent with the operational concept and safety management system applied to avoid ambiguity about the role and use of STCA.		
STCA-02	**Overall management of STCA**	**Organisational (ANSP)**
The ANSP ***shall*** assign to one or more staff, as appropriate, the responsibility for overall management of STCA.		
STCA-03	**Controllers training on STCA**	**Organisational (ANSP)**
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.		

STCA-04	Local instructions concerning use of STCA	Procedural (ANSP)
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.		

STCA-05	Controllers action in the event of an STCA	Procedural (ATCO)
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.*		

STCA-06	***Analysis of STCA performance***	***Procedural (ANSP)***
STCA performance ***shall*** be analysed regularly to identify possible shortcomings related to STCA.		

STCA-07	***Detection capability of STCA***	***Functional (STCA)***
STCA ***shall*** detect ~~and alert~~ operationally relevant conflicts involving at least one eligible aircraft.		
Related high-level requirement(s): STCA-07, STCA-08		
Rationale (based on PASS outcomes): The current text of STCA-07 (and STCA-08) is awkward. STCA-08 is either redundant because the need to alert is already stated in STCA-07 or contradictory to STCA-07 because it does not state that the alerts are limited to conflicts involving at least one eligible aircraft, which STCA-07 does. It is proposed to change the text of STCA-07 (and STCA-08) into a form similar to what was done in the specifications for MSAW [MSAW09].		

STCA-08	***Alerting capability of STCA***	***Functional (STCA)***
STCA ***shall*** ~~provide~~ alert~~s for~~ 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.~~*		
Related high-level requirement(s): STCA-07, STCA-08		
Rationale (based on PASS outcomes): The current text of STCA-08 (and STCA-07) is awkward. STCA-08 is either redundant because the need to alert is already stated in STCA-07 or contradictory to STCA-07 because it does not state that the alerts are limited to conflicts involving at least one eligible aircraft, which STCA-07 does. It is proposed to change the text of STCA-08 (and STCA-07) into a form similar to what was done in the specifications for MSAW [MSAW09]. The last sentence of the Note under STCA-08 is ambiguous. It could be interpreted as saying that the STCA designer could decide to not alert some operationally relevant conflicts. But operationally relevant conflicts are precisely those that have been decided to be worth alerting ("*covered by the adopted rule set and optimisation strategy*"). The true meaning of the last sentence is rather that there are inevitable limitations that will prevent some operationally relevant conflicts to be alerted. It is proposed to delete it to avoid any confusion.		

STCA-08a	***Alerting performance of STCA when conflict is operationally relevant***	***Performance (STCA)***
The number of operationally relevant conflicts alerted by STCA ***shall*** be kept to an effective maximum.		
Related high-level requirement(s): STCA-08, STCA-10, STCA-11		
Rationale (based on PASS outcomes): In the baseline requirements, there are qualitative performance requirements to minimize the number of nuisance (STCA-10) and false alerts (STCA-11), but not to minimize the number of not alerted operationally relevant conflicts. STCA designers should endeavour, as far as costs permit, to reduce the frequency of situations where ground-based technical issues would prevent the detection of an operationally relevant conflict. It is proposed to add the above requirement after STCA-08 to cover this gap.		

STCA-09	***Characteristics of STCA alerts***	***Functional (STCA)***
STCA alerts ***shall*** attract the controller's attention and identify the aircraft involved in the conflict; STCA alerts ***shall*** be at least visual. An audible element ***may*** be included to improve the systems ability to draw the controller's attention to the alert. If a continuous audible element is included, an acknowledgement mechanism ***may*** be provided to silence an alert.		

STCA-10	***Alerting performance of STCA when conflict is not operationally relevant***	***Performance (STCA)***
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.*		
STCA-11	***Alerting performance of STCA when there is no conflict***	***Performance (STCA)***
The number of false alerts produced by STCA ***shall*** be kept to an effective minimum.		
STCA-12	***Warning time performance of STCA***	***Performance (STCA)***
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.*		

STCA-13	***Continuity of STCA alerts***	***Functional (STCA)***
STCA ***shall*** continue to provide alert(s) as long as the alert conditions exist.		

STCA-14	***Possible inhibition of STCA alerts***	***Functional (STCA)***
STCA ***shall*** provide the possibility to inhibit alerts for predefined volumes of airspace and for individual flights. *Note.– It may be necessary to inhibit alerts for predefined volumes of airspace (e.g. exercise areas) to suppress unnecessary alerts. It may be necessary to inhibit alerts for individual flights (e.g. formation flights) to suppress unnecessary alerts.*		
STCA-15	***Information about STCA alert inhibitions***	***Functional (STCA)***
Alert inhibitions ***shall*** be made known to all controllers concerned.		
STCA-16	***Information about STCA status***	***Functional (STCA)***
Status information ***shall*** be presented to supervisor and controller working positions in case STCA is not available.		

STCA-17	***Availability of STCA data***	***Functional (STCA)***
All pertinent STCA data ***shall*** be made available for off-line analysis.		

B.3. Candidate additional operational requirements

B.3.1. The following additional operational requirements are derived from the PASS study outcomes.

OR-01	***Prevention of TCAS resolution advisories***	***Procedural (ATCO)***
When a time-critical avoiding instruction is deemed necessary in reaction to an STCA alert, the controller ***should*** use avoiding action phraseology to prompt pilot quick response. *Note: a prompt pilot quick response would have the positive side-effect of preventing the occurrence of TCAS resolution advisories.*		
Related high-level requirement: STCA-05		
Rationale (based on PASS outcomes): The monitoring activity (WA1) performed a descriptive statistical analysis of 180 conflicts, which demonstrated that "*the use of avoiding instruction phraseology allows an average gain of 3 seconds on the implementation of the manoeuvre*" by the pilot [D64]. The effect of this gain on the efficacy of the STCA to lead to an increase in separation has been demonstrated in the model-based performance evaluation (WA2) [W161]. In en-route, "*the effect of using avoiding phraseology when separation is already lost, or close to being lost, also become visible as the "standard" scenario shows a further decrease by 3% to 45% in the number of unaffected SC1 and SC2 encounters. Consequently, phraseology can have a significant positive impact on the outcome of the most critical losses of separation.* " In TMA, "*the effect of using avoiding phraseology when separation is already lost, or close to being lost, also become visible as the "standard" scenario shows a further decrease by 33% to 59% in the number of unaffected SC1 and SC2 encounter. […] Consequently, it confirms the potential significant positive impact that phraseology can have on the outcome of the most critical losses of separation.*"		

OR-02	***Compatibility between AIs and potential RAs***	***Procedural (ATCO)***

When an avoiding instruction is deemed necessary in reaction to an alert, the controller ***should*** 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.

Related high-level requirement: STCA-05

Rationale (based on PASS outcomes):

The possibility of incompatible AIs and RAs when issuing vertical avoiding instructions was identified in the operational safety assessment (WA4), with the following hazards and associated severity [D162]:

Operational Hazard	Severity
OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible	2
OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible	2
OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible	1
OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible	1

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.”*

OR-03	***Prevention of controller lack of attention***	***Functional (STCA)l***
STCA alerts ***may*** also attract the attention of controllers from adjacent sectors to allow them to warn the controller in which sector the alert is occurring.		
Related high-level requirement: STCA-09		
Rationale (based on PASS outcomes): The monitoring activity (WA1) [D64] found that "*looking at specific occurrences, the time taken by the controller to react to the alert appears to be influenced by the following: […]* • ***external intervention****: an avoiding instruction issued late […] may be the result of intervention by a third party, e.g. a controller from an adjacent sector phoning about a situation giving rise to concern"*		

OR-04	***Reduction of nuisance alerts through use of known/possible intents***	***Functional (STCA)***
STCA ***may*** 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. *Note: these aircraft manoeuvres complying with standard ATC procedures include the level-offs at a standard FL, the entry into a SID/STAR and the interception of an ILS.* *Note: taking into account information on actual or possible future aircraft trajectory will provide additional warning time in some specific operationally relevant conflicts (e.g. level-off at an occupied flight level).*		
Related high-level requirement: STCA-10		
Rationale (based on PASS outcomes): The model-based performance evaluation (WA2) demonstrated that **"***a feature common to all investigated STCA configurations is the issuance of unnecessary alerts in encounters with no loss of separation. The frequency of these unnecessary alerts can be reduced by a factor of 3 to 55, depending on the exact STCA implementation, either with use of the CFL or the SFL, or with less conservative separation and warning time parameter values*." ([D170]) Additionally, it was also highlighted that **"***for a given STCA system, the use of optional features (use of SFL/CFL, additional filters …) can provide additional warning time to the controller in a few specific circumstances*." ([D170])		

OR-05	***Alerting performance of STCA in terms of alert duration***	***Performance (STCA)***
When the geometry of the situation permits having sufficient warning time, the number of short duration alerts ***should*** be kept to an effective minimum. *Note: short duration alerts generally deactivate before a response by the controller could have taken effect. When the situation presents definite threat of separation loss, they are considered as late, i.e. ineffective to maintain or restore sufficient separation margins. When the situation presents little threat of separation loss, they are considered as undesirable.*		
Related high-level requirement: STCA-12		
Rationale (based on PASS outcomes): The model-based performance evaluation (WA2) demonstrated that "*"short duration" alerts are comparatively more frequent for the less conservative STCA families […] due to the use of reduced separation and warning time parameter values."* ([D170]) Additionally, it was also demonstrated that **"***the less conservative STCA families appear to be less effective than the other STCA families to help maintain (or restore) separation.*" ([D170]) Although not highlighted in the monitoring activity (WA1), the experience gained during the analysis of STCA-related occurrences tends to demonstrate that too many short duration alerts is likely to affect the controller confidence in STCA.		

OR-06	***Alerting performance of STCA in terms of alert continuity***	***Performance (STCA)***
The number of split alerts ***should*** be kept to an effective minimum.		
Related high-level requirement: STCA-13		
Rationale (based on PASS outcomes): In the model-based performance evaluation (WA2), "*the surveillance means was observed to potentially significantly affect the number of split alerts. Improving the quality of the surveillance data tend to limit these split alerts, and therefore, the quality of the alerts supplied by STCA to the controllers.*" ([D170]) Although not highlighted in the monitoring activity (WA1), the experience gained during the analysis of STCA-related occurrences tends to demonstrate that too many split alerts is likely to affect the controller confidence in STCA.		

B.4. Candidate quantitative performance requirements

B.4.1. 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 WA2. In order to give an insight into the rationale that led to the definition of these performance requirements, Table 9 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 10, 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 9: 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_mns	5 NM	800 ft	120 s

Table 10: Main STCA parameters for TMA and en-route airspace

PR-01	***Alerting capability of STCA depending on ANSP strategy***	***Performance (STCA)***

a) 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);

b) 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);

c) 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:

a) *When a liberal strategy is favoured, STCA are primarily designed to make a significant positive contribution to the effectiveness of collision prevention essentially.*
b) *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.*
c) *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.

Related high-level requirement(s): STCA-08

Rationale (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])

PR-02	***Acceptable minimum ratios of alerted separation infringements***	***Performance (STCA)***

a) When a liberal strategy is favoured, STCA ***shall*** produce alerts for at least 95% of initially "major", or worse, separation infringements;

b) 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;

c) 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.

Related high-level requirement(s): STCA-08a

Rationale (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, 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])

b) 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])

c) 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])

PR-03	***Acceptable maximum proportion of nuisance alerts***	***Performance (STCA)***
a) 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; b) 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; c) When a conservative strategy is favoured, STCA ***shall*** produce alerts in less than 80% of situations with no initial separation infringement.		
Related high-level requirement(s): STCA-10		
Rationale (based on PASS outcomes): The model-based performance evaluation (WA2) demonstrated that: a) The TMA *very_last_mn* and *about_very_last_mn* STCA configurations produce less than 80% of their alerts in conflicts with an SC3 to SC5 initial severity (i.e. conflict severity without controller avoiding instruction). The en-route *very_last_mn* and *beyond_last_mn* STCA configurations can also do so, although with additional optional features such as the use of a target FL (i.e. either CFL or SFL) and additional prediction filters. ([W168]) b) The TMA *beyond_last_mn* and *nearby_last_mn* STCA configurations produce less than 80% of their alerts in conflicts with an SC4 and SC5 initial severity (i.e. conflict severity without controller avoiding instruction). The en-route *almost_last_mn* STCA configuration can also do so, although with additional optional features such as the use of a target FL (i.e. either CFL or SFL) and additional prediction filters. ([W168]) c) The en-route *before_last_mn* and *last_two_mns* STCA configurations produce less than 80% of their alerts in conflicts with an SC5 initial severity (i.e. conflict severity without controller avoiding instruction). ([W168])		

PR-04	*Acceptable maximum proportion of late alerts*	*Performance (STCA)*

a) 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;

b) 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;

c) 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.

Related high-level requirement(s): STCA-12

Rationale (based on PASS outcomes):

The model-based performance evaluation (WA2) demonstrated that:

a) For 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, alerts produced in conflicts with an SC1 initial severity (i.e. conflict severity without controller avoiding instruction) enable to avoid the hazardous situation in more than 95% of cases, and alerts produced in conflicts with an SC2 initial severity enable to avoid the hazardous situation in more than 80% of cases. However, the use of horizontal avoiding instructions only does not enable the *very_last_mn* STCA TMA and en-route configurations to meet this requirement, which indicates that constraints should be put on the sense of controller avoiding instructions with these configurations. ([W168])

b) For the en-route *almost_last_mn* STCA configuration, as well as the TMA *beyond_last_mn* and *nearby_last_mn* STCA configurations, alerts produced in conflicts with an SC1 or SC2 initial severity (i.e. conflict severity without controller avoiding instruction) enable to avoid the hazardous situation in more than 95% of cases, and alerts produced in conflicts with an SC3 initial severity enable to avoid the hazardous situation in more than 80% of cases. However, the use of horizontal avoiding instructions only does not enable the *beyond_last_mn* STCA TMA configurations to meet this requirement, which indicates that constraints should be put on the sense of controller avoiding instructions with this configuration. ([W168])

c) For the en-route *before_last_mn* and *last_two_mns* STCA configurations, alerts produced in conflicts with an SC1 or SC2 initial severity (i.e. conflict severity without controller avoiding instruction) enable to avoid the hazardous situation in more than 95% of cases with an SC1 initial severity, alerts produced in conflicts with an SC3 initial severity enable to avoid the hazardous situation in more than 80%of cases and alerts produced in conflicts with an SC4 initial severity enable to avoid the hazardous situation in more than 50% of cases. ([W168])

PR-05	***Acceptable maximum ratio of short warning time alerts***	***Performance (STCA)***
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%.		
Related high-level requirement(s): STCA-12, OR-05		
Rationale (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 produce more than 80% of alerts with a warning time of 20 seconds or more before a loss of ATC separation minima, and consequently before the loss of half the ATC separation minima (corresponding to the hazardous situation considered by these STCA). The TMA *very_last_mn* and *about_very_last_mn* STCA configurations fail to provide such warning times before a loss of ATC separation minima, but would likely produce more than 80% of alerts with a warning time of 20 seconds or more before a loss of half the ATC separation minima. ([W168]) b) The en-route *almost_last_mn* and the TMA *nearby_last_mn* STCA configurations produce more than 80% of alerts with a warning time of 20 seconds or more before a loss of ATC separation minima, and consequently before the loss of 80% of the ATC separation minima (corresponding to the hazardous situation considered by these STCA). The TMA *beyond_last_mn* STCA configurations fail to provide such warning times before a loss of ATC separation minima, but would likely produce more than 80% of alerts with a warning time of 20 seconds or more before a loss of 80% of the ATC separation minima. ([W168]) c) The en-route *before_last_mn* and *last_two_mns* STCA configurations produce more than 80% of alerts with a warning time of 20 seconds or more before a loss of ATC separation minima (corresponding to the hazardous situation considered by these STCA). ([W168])		

PR-06	***Acceptable maximum ratio of short duration alerts***	***Performance (STCA)***
a) 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; b) 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; c) 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.		
Related high-level requirement(s): STCA-13		
Rationale (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, produce less than 20% of alerts lasting less than 20 seconds in conflicts with an SC1 or an SC2 initial severity (i.e. conflict severity without controller avoiding instruction). ([W168]) b) The en-route *almost_last_mn* STCA configuration, as well as the TMA *beyond_last_mn* and *nearby_last_mn* STCA configurations, produce less than 20% of alerts lasting less than 20 seconds in conflicts with an SC1, SC2 or SC3 initial severity (i.e. conflict severity without controller avoiding instruction). ([W168]) c) The en-route *before_last_mn* and *last_two_mns* STCA configurations produce less than 20% of alerts lasting less than 20 seconds in conflicts with an SC1, SC2, SC3 or SC4 initial severity (i.e. conflict severity without controller avoiding instruction). ([W168])		

B.5. Candidate quantitative safety requirements

B.5.1. The following safety requirements are derived from the PASS study outcomes and result from the operational safety analysis that has been conducted in WA4.

SR-01	***Correct implementation of STCA parameters for timeliness of alerts***	***Safety (STCA)***

The likelihood of an error in implementation of STCA parameter region ***shall*** be less than 9.7x10^{-5} per flight hour.

Related high-level requirement(s): STCA-02, SCTA-06, STCA-07, SCTA-08, STCA-12

Rationale (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.

Basic Event	Frequency	Operational Hazard
Event 43' 'Error in implementation of STCA parameter region causing late alert'	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

SR-02	***Adequate definition of STCA parameters for issuance of alerts***	***Safety (STCA)***
The likelihood of a lack of STCA alert due to tight parameters setting ('success case') ***shall*** be less than 2.1×10^{-4} per flight hour.		
Related high-level requirement(s): STCA-02, SCTA-06, STCA-07, SCTA-08, STCA-12		

Rationale (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.

Basic Event	Frequency	Operational Hazard
Event 56 'Lack of STCA alert due to tight parameters setting (success case)'	**2.1×10^{-4} / flight hour**	**OH1: Lack of ATCO instruction to solve a short-term conflict**
	2.3×10^{-2} / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
	5.4×10^{-3} / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
	9.0×10^{-3} / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
	1.9×10^{-3} / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
	5.9×10^{-3} / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

SR-03	***Availability of STCA service***	***Safety (STCA)***
The likelihood of having STCA out of service ***shall*** be less than 2.1×10^{-4} per flight hour.		
Related high-level requirement(s): STCA-02, SCTA-16		

Rationale (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'	**2.1×10^{-4} / flight hour**	**OH1: Lack of ATCO instruction to solve a short-term conflict**
	2.3×10^{-2} / flight hour	OH2: Late ATCO instruction to solve a short-term conflict – no interaction with TCAS RA
	5.4×10^{-3} / flight hour	OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible
	9.0×10^{-3} / flight hour	OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible
	1.9×10^{-3} / flight hour	OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible
	5.9×10^{-3} / flight hour	OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible

SR-04	***Acceptable rate of nuisance STCA alerts***	***Safety (STCA)***

The likelihood of an excessive nuisance STCA alert rate ***shall*** be less than $1.2x10^{-3}$ per flight hour.

Related high-level requirement(s): STCA-10

Rationale (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

SR-05	***Acceptable rate of false STCA alerts***	***Safety (STCA)***

The likelihood of an excessive false STCA alert rate ***shall*** be less than $1.2x10^{-3}$ per flight hour.

Related high-level requirement(s): STCA-11

Rationale (based on PASS outcomes):

The operational safety assessment (WA4) identified "*STCA – FALSE 'Excessive false 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 – 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

SR-06	*Correct implementation of STCA suppression list*	*Safety (STCA)*

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.

Related high-level requirement(s): STCA-02, STCA-06, STCA-07, STCA-08, STCA-12

Rationale (based on PASS outcomes):

The operational safety assessment (WA4) identified "*Event 25 'SSR code / flight ID erroneously inserted in the suppression list of STCA'*" 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
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

SR-07	*Correct design of STCA algorithm*	*Safety (STCA)*

The likelihood of an erroneous design of STCA algorithm ***shall*** be less than $9.7x10^{-5}$ per flight hour.

Related high-level requirement(s): STCA-02, STCA-06, STCA-12

Rationale (based on PASS outcomes):

The operational safety assessment (WA4) identified "*Event 27 'Erroneous design of STCA algorithm'*" 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 six OHs.

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

SR-08	***Correct implementation of STCA parameters for timeliness of alerts***	***Safety (STCA)***

The likelihood of a late STCA alert is issued due to erroneous parameters setting ***shall*** be less than $9.7x10^{-5}$ per flight hour.

Related high-level requirement(s): STCA-02, STCA-06, STCA-12

Rationale (based on PASS outcomes):

The operational safety assessment (WA4) identified "*Event 37 'Late STCA alert due to erroneous parameters setting*" 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 OH2 to OH6.

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
	$4.5x10^{-4}$ / 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

SR-09	***Adequate definition of STCA parameters for timeliness of alerts***	***Safety (STCA)***

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.

Related high-level requirement(s): STCA-02, SCTA-06, STCA-12

Rationale (based on PASS outcomes):

The operational safety assessment (WA4) identified "*Event 39 'Late 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 OH5. This basic event can be involved in all OH2 to OH6.

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
	$4.5x10^{-4}$ / 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

*** END OF DOCUMENT ***