







# Work Area 4 / Work Package 5 : Operational Safety Assessment Final Report

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

## PASS Project

Drafted by: Anne Damidau, Luca Save, Mathieu Sellier and Carlo Valbonesi

Authorised by: Béatrice Raynaud on 20/08/10

| **ADDRESSEES:** | **COPY TO:** |
|---|---|
| EUROCONTROL Participants,<br>DSNA Participants,<br>Deep Blue Participants,<br>QinetiQ Participants,<br>Egis Avia Participants. | - |

## RECORD OF CHANGES

| Issue | Date | Detail of changes |
|---|---|---|
| 0.1 | 23-06-2010 | Document Outline |
| 0.2 | 28-06-2010 | Update of the document accounting for internal comments |
| 0.3 | 20-08-2010 | Update of the document with result of fault trees analysis and safety requirements elaboration |
| 1.0 | 23-08-2010 | Final issue of the document |
| 1.1 | 10-09-2010 | Comments integration and conclusion redaction |

**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***

# TABLE OF CONTENTS

# ACRONYMS

| | |
|---|---|
| ACAS | Airborne Collision Avoidance System |
| ACC | Area Control Centre |
| AI | Avoiding Instruction |
| ANSP | Air Navigation Service Provider |
| ATC | Air Traffic Control |
| ATCO | Air Traffic Controller |
| ATCU | Air Traffic Control Unit |
| ATM | Air Traffic Management |
| DSNA | Direction des Services de la Navigation Aérienne |
| EHQ | EUROCONTROL Head Quarters |
| ESSAR | Eurocontrol SAfety and Regulatory Requirement |
| ET | Event Tree |
| FHA | Functional Hazard Assessment |
| LOS | Loss of Separation |
| N/A | Not Applicable |
| OHA | Operational Hazard Assessment |
| PASS | Performance and safety Aspects of Short-term Conflict Alert – full Study |
| Pe | Probability of Effects |
| PSSA | Preliminary System Safety Assessment |
| RA | Resolution Advisory |
| SO | Safety Objective |
| ST | Safety Target |
| STCA | Short Term Conflict Alert |
| SPIN | Safety nets Performance Improvement Network |
| TCAS | Traffic Alert and Collision Avoidance System |

WA Work Area

WP Work Package

# GLOSSARY

| | |
|---|---|
| Air Traffic Control Unit | A generic term meaning variously, area control centre, approach control unit or aerodrome control tower (PANS ATM 4444) |
| 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 | A conflict is a converging of aircraft in space and time which constitutes a predicted violation of a given set of separation minima, as per EUROCONTROL Specification for Short Term Conflict Alert. [REF 11] |
| 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. |
| Failure | The inability of any element of the Air Traffic Management System to perform its intended function or to perform it correctly within specified limits. (ESARR4 - [REF 14]) |
| Failure condition | A condition having an effect on the aircraft and/or its occupants, either directly or indirectly through loss of separation, which is caused or contributed to by one or more failures, or errors, considering flight phase and relevant adverse operational (density of air traffic, TMA etc…) or environmental conditions. (ESARR4 - [REF 14]) |
| Ground-based Safety net | A ground-based safety net is functionality within the ATM system that is assigned by the ANSP with the sole purpose of monitoring the environment of operations in order to provide timely alerts of an increased risk to flight safety which may include resolution advice [REF 11] |
| Hazard | Any condition, event, or circumstance which could induce an accident (ESARR4 - [REF 14])<br>In the qualitative analysis, hazard is more generically defined as a failure condition which could induce an incident or an accident ([REF 17]).<br>In the quantitative analysis a hazard is, in addition to the above definition, defined at the system boundary. |
| Near Mid-Air Collision | It is defined as an encounter during which at some time the horizontal separation of the two aircraft is less than 500ft and simultaneously the vertical separation of the aircraft is less than 100ft (cf. ASARP Project [REF 18]) |
| 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. (ESARR4 - [REF 14]) |
| Probability of Effects (Pe) | 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. |
| Short-term conflict | A potential infringement of separation minima that will occur in the short-term (e.g. within less than 2 minutes). |

# EXECUTIVE SUMMARY

As part of PASS project, an operational safety assessment has been conducted to address the safety aspects of joint STCA and TCAS operations. This assessment includes hazard identification, risk assessment and mitigation means determination as required by ESARR 4. The work was performed in two steps:

- Step 1: Preliminary operational safety assessment (Phase 2). This step was realised in 2009 and already presented in [REF 7].
- Step 2: Consolidated operational safety assessment and requirement determination (Phase 3).

Step 1 of this safety assessment was conducted in three stages, which are detailed below:

- A preliminary hazard identification (qualitative analysis): the objectives of this study were to identify a preliminary list of basic types of hazards based on the analysis of real ATC incidents studied in WA1 of PASS Project and integrated with inputs from other studies, such as those promoted by the SPIN Task Force.
- A preliminary event tree analysis (quantitative analysis): the main objective of this study was to derive preliminary safety objectives based on the results of previous qualitative analysis as required by ESARR4 [REF 14].
- A summary and comparison of the qualitative and quantitative analyses: the objectives were to provide the results of both studies and to compare them.

The following improvement fields / activities were undertaken in Phase 3 of PASS Project and concern the consolidation of Phase 2 material:

- Harmonize the severity results in both analyses. This also implied the need to revisit the definition of some hazards.
- Validate / refine the barriers identified for each hazard in the quantitative safety analysis by operational experts or simulations and the assigned severity classes.
- Refine the probabilities of success/failures of some identified barriers.

Then, the main activity of Phase 3 consisted in determining how the system architecture (encompassing people, procedures, equipment) could be made safe, and as such in deriving safety requirements.

This has been achieved by developing fault trees based on a generic high-level architecture in order to identify the causes and combination of causes leading to each hazard. After the identification of the hazards causes, the next step consisted in allocating the quantitative safety objectives and in deriving quantitative safety requirements. This activity was confined to the STCA system and associated ‘technical’ procedure(s). Assumptions were defined for elements external to STCA (such as surveillance inputs to STCA), as well as on controller or pilot behaviour. No qualitative requirements such as on procedures validation or human training have been developed.

# 1. Introduction

## *1.1. PASS Project*

1.1.1. PASS (**P**erformance and Safety **A**spects of **S**TCA – Full **S**tudy) is a EUROCONTROL project with the objective to study performance and safety aspects of Short Term Conflict Alert (STCA), including human performance aspects and consideration of interactions between operational use of STCA and Airborne Collision Avoidance System (ACAS) [REF 1]

1.1.2. The fourth Work Area (WA4) of the PASS project specifically addresses the safety aspects of STCA. Both qualitative and quantitative safety analyses are performed with a specific focus on the identification and assessment of operational factors, in addition to the environmental and technical factors, which may influence the safety of joint STCA and ACAS operations.

1.1.3. The work is planned to be conducted in two steps:

- Step 1: Preliminary operational safety assessment (Phase 2); and
- Step 2: Consolidated operational safety assessment and requirement determination (Phase 3).

## *1.2. Safety Context*

1.2.1. As the name suggests, the sole aim of a ground-based safety net is to positively contribute to the safety of the ATM system. In the EUROCONTROL STCA specification document [REF 11], the STCA is given the following definition: “It is 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”. It is also recalled that its “presence is ignored when calculating capacity” as well as efficiency.

1.2.2. As per SRC28.06 policy [REF 24], ground-based safety nets are now confirmed being part of the ATM system and they are, as such, subject to hazard identification, risk assessment and mitigation as required by ESARR 4. Indeed the real-time use of ground based safety nets can have unintended negative effects. They can induce new hazards, or degrade effects of existing hazards.

1.2.3. In particular, this policy indicates that the risk assessment and mitigation process for ground based safety nets should consider interaction between ground-based safety nets and similar airborne functions.

1.2.4. This safety assessment is focusing on the potential negative effects of STCA with TCAS. On the other hand, the mitigation by airborne safety nets of STCA-related hazards effects is not to be accounted for.

## *1.3. Operational Safety Assessment Objective*

1.3.1. The operational safety assessment seeks to identify the errors and malfunctions of the ATM system which are related to the functioning of STCA or to the interoperability aspects of STCA and TCAS analyzed as an overall concept. The identified hazards are then used to derive safety objectives, as a first step for the identification of Safety Requirements and Recommendations in PASS Phase 3.

1.3.2. The EUROCONTROL ANS Safety Assessment Methodology [REF 13] (SAM) identifies the need for "success" approach and "failure" approach to safety assessment[1]. The "success" case covers the reduction in risk of accident to air traffic that would otherwise exist, afforded by the desired functional and performance properties of the ATM system. On the other hand, the "failure" case covers the mitigation of anomalous behaviour of the ATM system that could induce a risk that would otherwise not have arisen.

1.3.3. The objective of the operational safety assessment in WA4 is to address the "failure" approach. The "success" approach (prevention of accidents) was covered during the PASS fast-time simulations which took place in Phase 3, as it is intended: "to compare the "initial" severity of the encounter without the effect of the controller's instruction prompted by STCA and the "final" severity resulting from the pilot's response to the controller's instruction" (see [REF 6]).

1.3.4. Step 1 of this operational safety assessment in Phase 2 of the PASS Project was conducted in three stages:

- **Preliminary hazard identification (qualitative analysis)**: the objectives of this study were to identify a preliminary list of basic types of hazards based on the analysis of real ATC incidents studied in WA1 of PASS Project and integrated with inputs from other studies (see [REF 15] and [REF 16]), such as those promoted by the SPIN Task Force. Then for each of these basic types of hazards, operational scenarios were defined and were discussed in a workshop with operational experts, in order to assess the severity of their operational consequences and to identify possible further basic types of hazards with relevance for the study of the STCA-TCAS overall concept. The detailed analysis is provided in a separate document [REF 17]

- **Preliminary event tree analysis (quantitative analysis)**: the main objective of this study was to derive preliminary safety objectives based on the results of previous qualitative analysis as required by ESARR4 [REF 14]. 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. The method consisted in developing event trees, which are graphical means that enable to identify and quantify all possible outcomes of the hazards. The detailed analysis is provided in a separate document [REF 5].

[1] However, SAM currently does not provide much guidance on what the success case entails.

- **Summary and comparison of the qualitative and quantitative analyses**: the objectives are to provide the results of both studies and to compare them. The identification of future steps to be performed in Phase 3 of PASS Project, including the improvement areas, is also addressed. The summary and comparison are provided in the present document.

1.3.5. Step 2 of this operational safety assessment has consisted of:

- **Consolidated event tree analysis (quantitative analysis),** which included a refinement of operational hazards (see more details in [REF 8]) and the refinement of some assumptions defined in [REF 5]). The consolidated event tree analysis contains the determination of consolidated safety objectives per operational hazards [REF 9].

- **Preliminary fault tree analysis (quantitative analysis)** which permitted to derive safety requirements for STCA based on the safety objectives defined in the consolidated Event Tree Analysis. For that purpose, fault trees were developed based on the refined list of operational hazards. Fault trees were elaborated by decomposing the hazard in a combination of failures (a top-down approach is adopted) linked by different gates: "AND" gates and "OR" gates (see more details in [REF 10]).

- **Safety requirements determination:** 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 (see more details in [REF 10]).

## *1.4. Document Overview*

1.4.1. The objective of this document is to present a summary of all safety activities (Step 1 and Step 2) that were performed during PASS project.

1.4.2. First objective in section 2 is to present the operational/functional hazard assessment (OHA/FHA) performed in both Step 1 and Step 2: it provides the initial – Step 1 – and the consolidated – Step 2 – hazards list, and describes how hazards' effects were assessed to permit safety objectives derivation.

1.4.3. In PASS project, this event trees analysis was selected to assess the operational effects of hazards in order to define safety objectives to hazards, as required by ESARR4 [REF 14]. 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.

1.4.4. The basis for the consolidation activity performed in Step 2, was the refinement of operational hazards (see more details in [REF 8]) and the refinement of some assumptions defined in [REF 5])

1.4.5. Afterwards, section 3 presents the preliminary system safety assessment (PSSA): it describes how fault trees were developed to derive safety requirements to STCA based on the safety objectives defined in the consolidated Event Tree Analysis [REF 9] and how probability for each basic event was determined thanks to fault tree analysis [REF 10]. This section also provides all safety requirements done on STCA system thanks to the fault tree analysis.

# 2. Operational / Functional Hazards Assessment (OHA / FHA)

## *2.1. Operational Safety Assessment Scope*

2.1.1. **The preliminary hazard identification (qualitative analysis)** [REF 17] pointed out the potential errors and malfunctions of the ATM system which are related to the functioning of STCA or to the interoperability aspects of STCA and TCAS analyzed as an overall concept. The study did not investigate the hazards related only to TCAS. These are considered out of the scope of the PASS project and have been already covered by other safety studies, such as those made in the context of the IAPA [REF 27], ACASA [REF 28] and ASARP [REF 18] projects.

2.1.2. The diagram in Figure 1 represents the area of interest of the analysis delimited by the light grey area, which excludes the part of the nominal sequence only referred to TCAS. It is a combination of the STCA and TCAS loops, and is aimed at depicting the nominal sequence of events in case of activation of a TCAS RA.

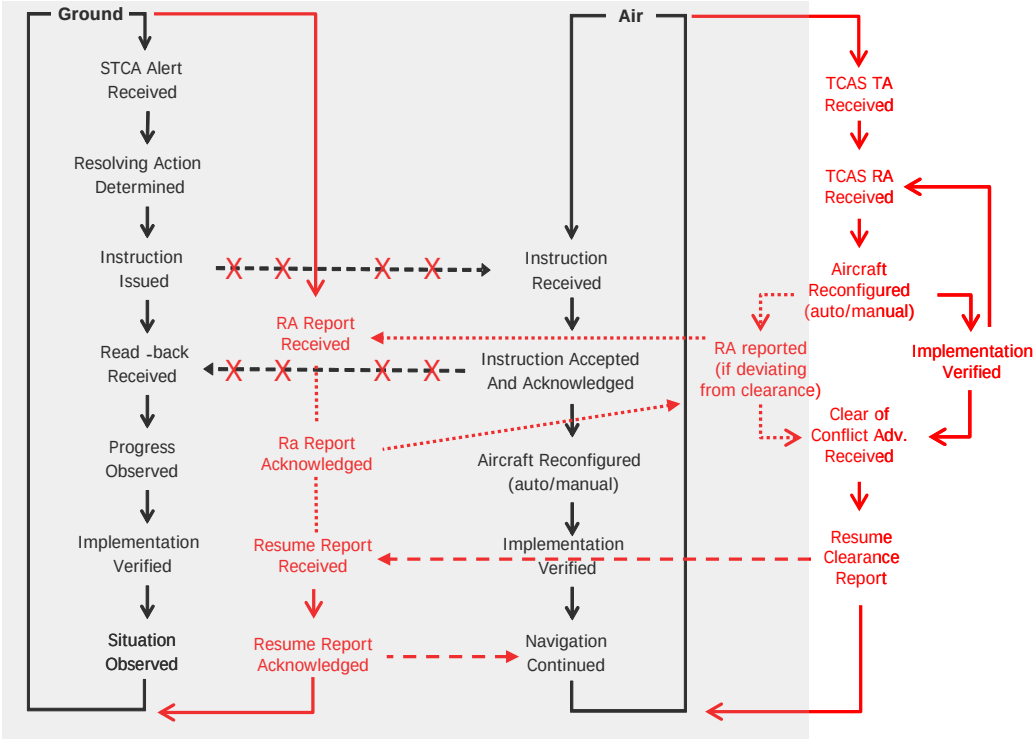



**Figure 1: The transition between STCA and TCAS control loops in case of TCAS RA**

2.1.3. In the **preliminary event tree analysis (quantitative analysis)** [REF 5], the part of the ATM system under assessment comprises the controller(s) assisted by STCA to prevent collision between aircraft. The difference with the qualitative analysis is that in the quantitative study, pilots are considered external to the system under assessment. When controllers' avoiding instructions are issued, the presence or not of STCA in assisting controllers is assumed not to influence pilots' manoeuvres. Meanwhile the pilots' behaviour to controllers' instructions (either by implementing or not the ATC instructions) is considered in the event trees during the effects analysis of the hazards.

2.1.4. Next figure illustrates the system under assessment considered in the quantitative analysis [REF 5] (STCA and controllers' actions triggered by STCA in the grey boxes) interacting with other external components in a given operating environment (En-route or TMA). External components encompass pilots' related actions after receiving an avoiding instruction. Note that technical aspects related to STCA, i.e. the components providing information to STCA to generate alerts such as the Surveillance Data Processing, Environment Data Processing and Flight Data Processing, have not been illustrated in this figure.

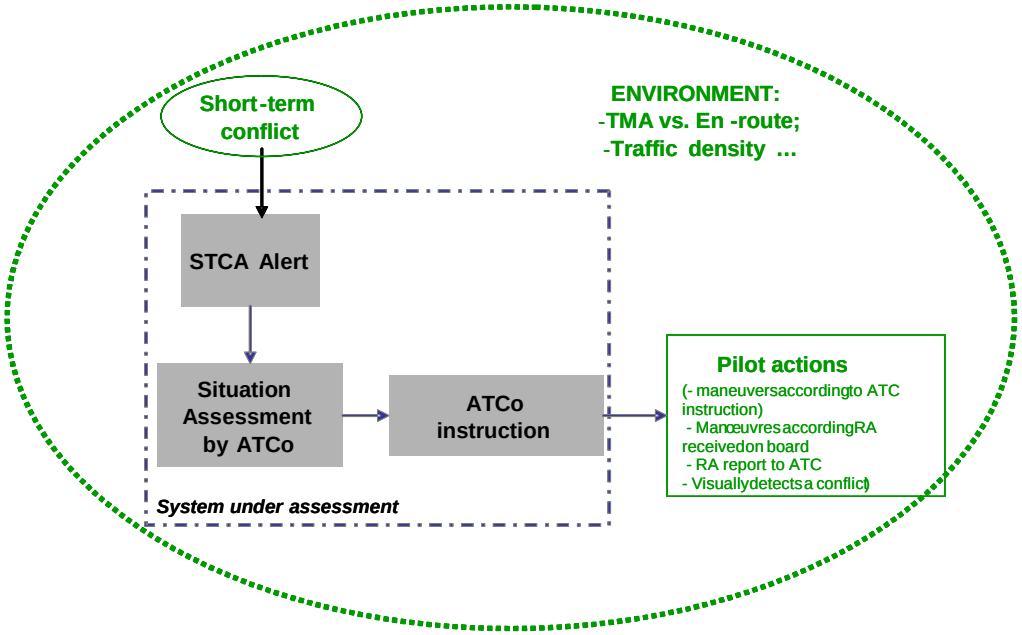



**Figure 2: Boundaries of the System under Assessment**

## *2.2. Step 1 - Identification of Basic Types of Hazards*

2.2.1. Based on the analysis of ATC incidents extracted from the "Analysis of real ATC Incidents" (WA1-WP4), [REF 2], the study has first identified 20 basic types of hazards, classified into the following 7 main categories:

- STCA vs Conflict
- ATC vs STCA
- ATC vs TCAS
- Crew vs ATC Avoiding Instruction
- Crew vs TCAS
- Crew vs RA Report
- STCA vs TCAS.

2.2.2. The list of these basic types of hazards is provided in ANNEX B: Basic types of hazards.

2.2.3. The study has then elaborated a list of 57 detailed scenarios, based on a combination of same basic hazards with different contributing factors. Refer to PASS – Operational Safety Assessment Interim Report, [REF 7]

## 2.3. Step 1 - Initial List of Operational Hazards

2.3.1. The basic types of hazards defined in the previous qualitative analysis [REF 17], have been identified at different levels. They map onto the system as shown in the Figure 3 below.

2.3.2. According to EUROCONTROL SAM (Safety Assessment Methodology, FHA – Chapter 3) they should be defined at the boundary of the ATM system under assessment with the environment / external systems in order to be as close as possible to the operations.

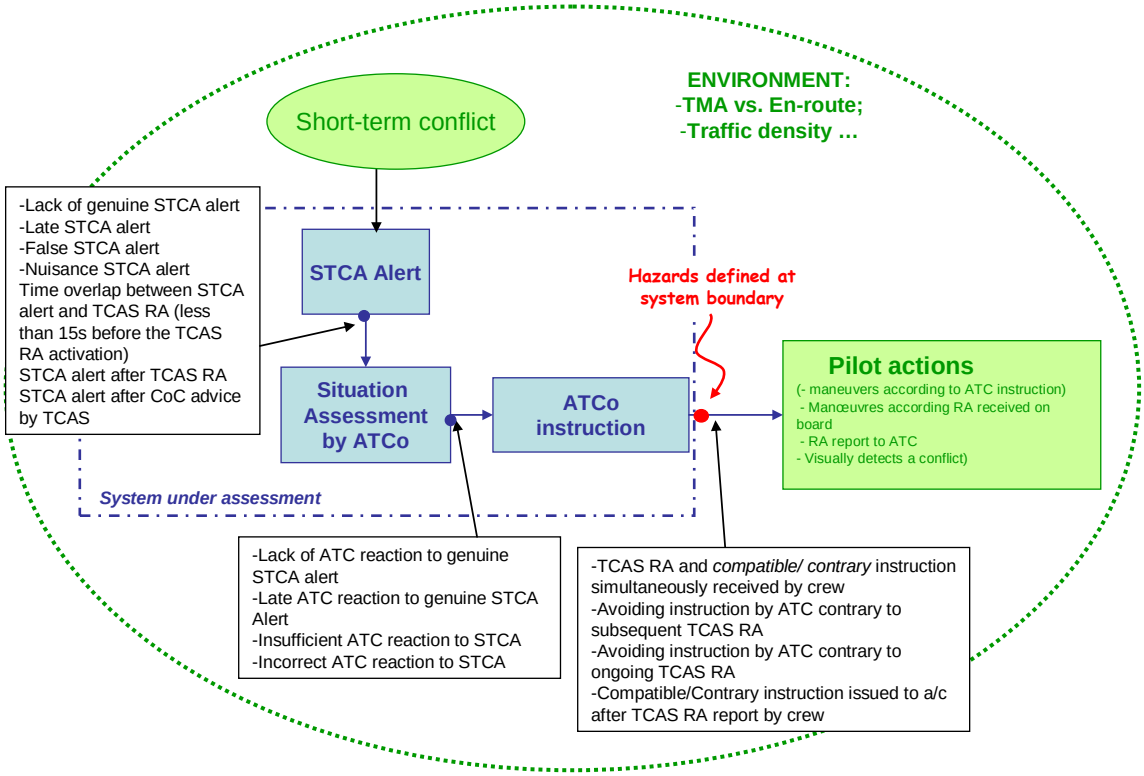



**Figure 3 : Failures and Hazard Identification Level**

2.3.3. Hence, the following hazards have been defined at the level of “ATCO instruction”:

| Initial Hazard Title | Initial Hazard Definition |
|---|---|
| *OH1: Lack of ATCO instruction to solve a short-term conflict* | The ATCO does not issue any avoiding instruction, although there is a real short-term conflict with Loss of Separation (LOS) (See qualitative safety analysis [REF 17], §3.4.4). |
| *OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA* | The ATCO issues an avoiding instruction with delay such that he/she cannot prevent LOS but with time prior to a potential TCAS RA. |
| *OH3: Avoiding instruction by ATCO received shortly before TCAS RA* | The ATCO - unaware of the TCAS RA that the crew is going to receive - issues an avoiding instruction (See qualitative safety analysis [REF 17], §3.4.9) |
| *OH4: TCAS RA and ATCO instruction simultaneously received by crew* | The ATCO - unaware of the imminent TCAS RA - issues an avoiding instruction which is received by the crew at about the same time as the TCAS RA (See qualitative safety analysis [REF 17], §3.4.9). |
| *OH5: Avoiding instruction by ATCO received after an ongoing TCAS RA* | The ATCO issues an avoiding instruction while the flight crew has already received a TCAS RA (See qualitative safety analysis [REF 17], §3.4.9). |
| *OH6: Insufficient ATCO instruction to solve a short-term conflict* | The ATCO issues an avoiding instruction to solve a short-term conflict, which does not allow to maintain or restore separation (See qualitative safety analysis [REF 17], §3.4.4). |
| *OH7: Incorrect ATCO instruction to solve a short-term conflict* | The ATCO issues a corrective instruction to solve a short-term conflict that leads to a reduction of the safety margins instead of an increase (See qualitative safety analysis [REF 17], §3.4.4). |

**Table 1: Initial List of Hazards retained for the Preliminary Event Tree Analysis**

## *2.4. Step 2 – Consolidated List of Operational Hazards*

2.4.1. In the context of WP2 (Consolidated Operational Hazard Analysis) in step 2, the list of hazards described above was partially reviewed based on expert judgment, on the analysis of other ACAS-related studies [REF 20] and on a deeper understanding of cognitive aspects related to the performance of pilots and controllers.

2.4.2. In some cases the hazards were modified in their definition to reflect a different structure of the corresponding event tree. In other cases the hazards originally proposed were split in to two different hazards in order to represent different operational situations. Finally other hazards were excluded from the overall list and considered already covered by other hazards.

2.4.3. The following section summarizes all the changes and their rationale, while the table in the final Section 3 presents the consolidated list and the relations with the original hazards.

2.4.4. **OH1** and **OH2**, respectively "Lack of ATCO instruction to solve a short-term conflict" and "Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA" remained unchanged.

2.4.5. **OH3** and **OH4**, respectively "Avoiding instruction by ATCO received shortly before TCAS RA" and "TCAS RA and ATCO instruction simultaneously received by crew" have undergone similar modifications, including:

- The **incompatibility between AI and TCAS RA has become a defining element of the OH** and not just a barrier as in the previous version.
- All **cases in which AI and TCAS RA are compatible are not considered** anymore among the hazards;
- A **distinction between en-route and TMA areas** has been added.

2.4.6. As far as the third modification is concerned (third bullet above), the analysis of recent studies [REF 20] put in evidence that the lower the level at which aircraft are flying, the lower is the pilot compliance rate to RAs. Particularly the monitoring of three major European TMAs for a significant period showed an average rate of pilot's compliance to RAs of about 60%. While in the Preliminary Event Tree Analysis [REF 5] – which assumed ACAS related events to occur only in en-route environments – this rate was fixed to 90%. Actually the data monitored in TMA are influenced by several factors which are generally not part of the core of the PASS project, such as the role played by non-controlled aircraft, by VFR and by TCAS-unequipped aircraft. Nevertheless it was deemed necessary to distinguish the rate of pilot compliance to RA in at least two broad categories.

2.4.7. The three modifications described above led to convert the original hazard OH3 into OH3 and OH5, and the former OH4 into OH4 and OH6.

| Initial OH | New OH |
|---|---|
| **OH3** - AI before RA | **OH3** (→ en-route) |
| | **OH5** (→ TMA) |
| **OH4** - AI simultaneous to RA | **OH4** (→ en-route) |
| | **OH6** (→ TMA) |

2.4.8. Finally the original **OH5**, "Avoiding instruction by ATCO received after an ongoing TCAS RA" has been removed from the list of hazards under assessment. This situation has been considered already covered by other hazards.

2.4.9. The former OH6 and OH7, respectively “Insufficient ATCO instruction to solve a short-term conflict” and “Incorrect ATCO instruction to solve a short-term conflict” have been retained with the original definition. Nonetheless they are neither further analyzed in the Event Tree Analysis nor in the Fault Tree Analysis as they are not expected to bring any specific requirement.

| Consolidated Hazard Title | Consolidated Hazard Definition | Rationale |
|---|---|---|
| *OH1: Lack of ATCO instruction to solve a short-term conflict* | The ATCO does not issue any avoiding instruction, although there is a real short-term conflict with Loss of Separation (LOS) | - Same as former OH1 |
| *OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA* | The ATCO issues an avoiding instruction with delay such that he/she cannot prevent LOS but with time prior to a potential TCAS RA. | - Same as former OH2 |
| OH3: Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible | The ATCO, unaware of the TCAS RA that the crew is going to receive, issues an avoiding instruction in opposite direction to the subsequent TCAS RA. The time delay between the AI and the RA is sufficient for the pilot to start an avoiding manoeuvre[2]. The hazard occurs in an en-route airspace. | - Similar to former OH3<br>- Incompatibility between AI and TCAS RA added<br>- Specification of en-route airspace location added |
| OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible | The ATCO -unaware of the imminent TCAS RA- issues an avoiding instruction which is received by the crew at about the same time as the TCAS RA but in opposite direction. The hazard occurs in an en-route airspace. | - Similar to former OH4<br>- Incompatibility between AI and TCAS RA added<br>- Specification of en-route airspace location added |
| OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible | The ATCO, unaware of the TCAS RA that the crew is going to receive, issues an avoiding instruction in opposite direction to the subsequent TCAS RA. TCAS RA. The time | - Similar to former OH3<br>- Incompatibility between AI and TCAS RA added |

[2] Note that in this context the time delay is referred to the possibility for the pilot to start implementing a manoeuvre and does not imply that the manoeuvre is actually implemented.

| Consolidated Hazard Title | Consolidated Hazard Definition | Rationale |
|---|---|---|
| | delay between the AI and the RA is sufficient for the pilot to start an avoiding manoeuvre[3]. The hazard occurs in a TMA airspace | - Specification of TMA location added |
| OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible | The ATCO -unaware of the imminent TCAS RA- issues an avoiding instruction which is received by the crew at about the same time as the TCAS RA but in opposite direction. The hazard occurs in a TMA airspace | - Similar to former OH3<br>- Incompatibility between AI and TCAS RA added<br>- Specification of TMA location added |
| *OH7: Insufficient ATCO instruction to solve a short-term conflict* | The ATCO issues an avoiding instruction to solve a short-term conflict, which does not allow to maintain or restore separation. | - Same as former OH6 |
| *OH8: Incorrect ATCO instruction to solve a short-term conflict* | The ATCO issues a corrective instruction to solve a short-term conflict that leads to a reduction of the safety margins instead of an increase. | - Same as former OH7 |

**Table 2 : Consolidated List of Hazards**

[3] See note 1.

## *2.5. Hazards Effects Assessment*

2.5.1. As already said before, hazards effects have been assessed by way of event trees. In an event tree diagram, each branch level describes a barrier. The trees are typically built on a binary accounting for the “success” or “failure” of the barrier or mitigation means in becoming effective. At the end of each branch, the effects of the hazards have been assessed along with the corresponding Severity Class as per ESARR4 [REF 14], and the probability that the hazard generates that effect (“Pe”) is calculated based on the success/failure probability of each concerned barrier. An example of Event Tree is provided in annex D.

2.5.2. Barriers of hazards represented in the event trees are mitigation means that help in detecting and recovering from a hazard. These barriers hence are intended to reduce the hazard operational effects and/or their occurrence. It is recognised that there exist barriers that prevent the hazard from occurring, which are not addressed in this paper. The current safety assessment concentrates on hazard effects and assumes the hazard has already occurred.

2.5.3. In general barriers are external to the system under assessment and correspond to procedural and environmental factors. A list of *Environmental Conditions (EC)* and *External Mitigation Means (EMM)* are then derived from this assessment. They are expressed in the form of a requirement or an assumption depending on the nature of the mitigation means.

2.5.4. Note that the *Environmental Conditions (EC)* are elements of the environment such as the type of airspace, traffic density, and that they can also aggravate the effects of the hazards.

2.5.5. Concerning the External Mitigation Means (EMM) they are procedures that mitigate hazards’ effects.

2.5.6. It is recalled that as recommended by ED125 [REF 22] barriers that shall be excluded from the risk mitigation strategy are:

- Airborne Safety Nets;
- Mitigation means that have already been taken into account as internal to the system under assessment.

2.5.7. Afterwards, the efficiency of each barrier has been determined. It corresponds to a quantitative probability of success or failure of the barrier. These probabilities have been obtained from other projects, such as ASARP [REF 18], FARADS, from safety engineering judgement, from WA1 documents (Monitoring of ATC incidents, using results from “Analysis of SNET performance based on monitoring data” PASS document (doc 64) [REF 3], “Descriptive analysis of observed SNET performance” PASS document (doc 90) [REF 4], etc.) and some others from initial values from WA2.

## *2.6. Safety Objectives Derivation*

2.6.1. One main input for the calculation of the Safety Objectives are the safety targets apportioned to the System under assessment.

2.6.2. 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. The detailed process developed to derive these Safety Targets is explained in annex A of this document.

| Severity Class | Safety Target [per flight hour] |
|---|---|
| 1 | 3.0E-09 |
| 2 | 3.0E-06 |
| 3 | 3.0E-05 |
| 4 | 3.0E-03 |

**Table 3: Apportionment of ATM Safety Targets to be considered**

2.6.3. For each hazard and each possible severity class, Safety Objectives (SO) have been calculated based on the Safety Targets (ST), the probability of effects (Pe), i.e. the probability that the hazard will lead to operational effects of this severity class, and the number of hazards identified for this severity class, using the following formula:

2.6.4. $SO_i = \frac{ST_i}{Pe_i \times N_i}$, where i corresponds to each Severity Class (i from 1 to 4), Pei is the probability for the hazard to have a severity SCi and Ni corresponds to the number of hazards having credible effects in that severity class i.

2.6.5. Finally, the safety objective derived to each hazard corresponds to the most stringent frequency determined by the above formula. This Safety Objective is then retained as input to the subsequent Fault Tree Analysis for each hazard. It is a simple way to directly ensure that if the most stringent safety objective is met for each hazard, then the other less stringent safety objectives of the remaining severity classes will be consequently met.

2.6.6. It is assumed that the same number of hazards apply in En-Route and in TMA as provided in the following table. Therefore for each Severity class Ni is equal to 6 in both types of airspace.

| Hazards in En-Route | Hazards in TMA |
|---|---|
| OH1 | |
| OH2 | |
| OH3 | |
| OH4 | |
| | OH5 |
| | OH6 |
| *OH7* | |
| *OH8* | |
| **Total number of hazards: 6** | **Total number of hazards: 6** |

**Table 4 : Number of Hazards per Airspace**

2.6.7. This table below provides a summary of the severity, the probability of effects (Pe values) and Safety Objective (SO) for each hazard.

2.6.8. 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 SO 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., one 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).

| Hazard | Severity | Pe Value | Safety Objective [Per flight.hour] | SO / ATSU -1 100 000 flight hours per year | SO / ATSU -2 500 000 flight hours per year |
|---|---|---|---|---|---|
| OH1: Lack of ATCO instruction to solve a short-term conflict - no interaction with TCAS RA | 2 | 6.0E-02 | 8.3E-06 | 0.8 event every year | 4 events every year |
| OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA | 3 | 1.1E-02 | 4.5E-04 | 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 | 2 | 6.9E-02 | 7.2E-06 | 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 | 2 | 5.7E-02 | 8.8E-06 | 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 | 2/1 | 1.3E-01 (sev 2)<br>1.3E-04 (sev 1) | 3.8E-06<br>3.8E-06 | 0.4 event every year | 2 events every year |

| Hazard | Severity | Pe Value | Safety Objective [Per flight.hour] | SO / ATSU -1 100 000 flight hours per year | SO / ATSU -2 500 000 flight hours per year |
|---|---|---|---|---|---|
| OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible | 1/2 | 8.5E-05 | 5.8E-06 | 0.6 event every year | 3 events every year |

**Table 5: Safety Objectives Results**

2.6.9. For OH5 and OH6 the two severity classes 1 and 2 tend to provide the most credible effects.

2.6.10. Safety objectives values are provided with one decimal but it is recognised that these results are not so precise as these values are built upon assumptions that are based on expert judgement or statistical data.

2.6.11. These Safety Objectives are quite demanding but note that the likelihood of occurrence of short-term conflicts is included in the likelihood of occurrence of each hazard, e.g. there is a need to combine the probability of having a conflict and the ATCO not to intervene for OH1 to occur (either ATCO does not intervene to a genuine STCA Alert or lack of genuine STCA alert and ATCO does not detect there is a short-term conflict).

2.6.12. Also note that these demanding Safety Objectives are derived from the risk mitigation strategy applied, which excludes pure luck and the airborne safety net from the barriers that can mitigate the effects of the hazards.

2.6.13. Finally the interaction between the prevention of collision by ATCOs assisted by STCA and the airborne safety net, i.e. TCAS, is explored through the analysis of OH3 to OH6 effects and related Safety Objectives.

# 3. Preliminary System Safety Assessment - PSSA

## *3.1. Logic Design Description*

3.1.1. Across Europe, the STCA system is composed of common algorithms used to detect conflicts but individual implementations use various STCA parameter values. Some additional features are present in only some existing STCA systems.

3.1.2. The inputs to and outputs from the reference STCA system are presented in the STCA context diagram and is extracted from the EUROCONTROL Guidance Material for Short Term Conflict Alert- Appendix A: Reference STCA System [REF 19]:

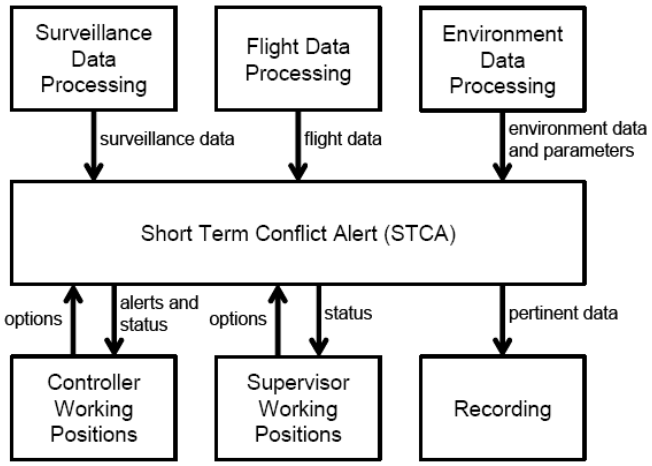



**Figure 4 : STCA interface with external devices**

3.1.3. As illustrated in the figure above, STCA should obtain information from Surveillance Data Processing, from Environment Data Processing and possibly from Flight Data Processing in order to generate alerts [REF 19]:

- Surveillance data including tracked pressure altitude information should be used to predict conflicts
- Flight data should be used as follows:
  - Type/category of flight: to determine the eligibility for alert generation
  - RVSM status: to apply appropriate parameters in RVSM airspace
  - Concerned sector(s): to address alerts
  - Cleared/Block Flight Levels: to increase the relevance of conflict prediction
  - Type of aircraft/wake turbulence category
  - Number of aircraft: to apply appropriate parameters for formation flights

- Manually entered Flight Levels: to compensate for missing pressure altitude information

– Environment data and parameters should include parameters to configure STCA for distinct volumes of airspace

3.1.4. Various optional features exist, and the most relevant ones for this safety analysis concern the use of CFL or SFL to predict conflicts appearing on the vertical plane.

3.1.5. Other STCA features can affect the detection of conflicts on the horizontal plane. These include current proximity filter and turning prediction filter [REF 19].

3.1.6. The last main option concerns the Multi-Hypothesis Feature applied in specific geographic area (based on the knowledge of the local ATC procedure).

3.1.7. In the frame of PASS, during the fault tree analysis and during the safety objectives allocation three different configurations of STCA were considered:

- First, STCA does not use any filter (OPTION 1)
- Second, STCA only uses CFL filter (OPTION 2)
- Third, STCA uses all available filters (CFL, SFL, Multi Hypothesis Features, Proximity Filter and Turning Prediction Filter) - (OPTION 3)

## *3.2. Fault Trees Development*

3.2.1. Fault trees were developed based on the refined list of operational hazards presented in the 'Consolidated List of Operational Hazards' document (paper 151) [REF 8].

3.2.2. Fault trees were constructed by decomposing the 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).

3.2.3. In the fault trees, several kinds of basic events were combined to lead to the hazard. Those different kinds of basic events are presented hereafter:

- Basic event could be human failure to operate a basic task such as conflict detection for ATCo, or ATCo instruction execution for a Pilot.
- Basic event could be an external event to the STCA system (technical or not) like "Two A/C are on collision course" or "Transponder failure"
- Basic event could be an internal STCA failure like 'Erroneous design of STCA algorithm'
- Basic event could also be a conditional event like 'STCA use SFL' or 'STCA does not use current proximity filter'. Value of this kind of event could be 0 or 1 depending on the STCA configuration.

## *3.3. Basic Causes Probability Determination*

3.3.1. Safety objective 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.
- A bottom-up allocation process: it consists in assigning a probability to each basic event based on engineering judgement.

3.3.2. Probability concerning an external event, or an external failure (e.g.: Two A/C are on collision course, 'Radar Processing Failure'….) was determined based on statistical studies performed through simulations, or events reporting (e.g. [REF 23]), or based on engineering judgement. All these values were taken as assumptions. When an event is used in several fault trees, its probability is always the same. An illustration of this process is presented in annex C, §5.14.5.

3.3.3. Probability concerning a human failure (e.g.: Lack of ATCO detection of a short term conflict – no STCA) was determined based on statistical studies performed through simulations or events reporting (e.g. [REF 23], [REF 25]); or based on engineering judgement. All these values were taken as assumptions. When a human failure is used in several fault trees, its probability is always the same. An illustration of this process is presented in annex C, §5.14.5.

3.3.4. The three “selected” configurations of STCA have an impact in the occurrence of OH2. Indeed depending on the option implemented in STCA, some type of vertical or horizontal conflict geometry might be detected at the earliest opportunity (does not lead to OH2) or with delay (leads to OH2). Safety objective of OH2 was apportioned to these various configurations, and the most stringent one, i.e. OPTION 1 (no option), derived the most stringent safety requirements to STCA.

## *3.4. Quantitative Safety Requirements Derivation*

3.4.1. During this study certain events were present in more than one fault tree. To express a safety requirement applicable to all fault trees, the most stringent ‘apportioned’ safety objective for each event was taken into account and used in all the trees where that event appeared (see [REF 10] for more details).

3.4.2. For example, if you consider Event 39 ‘Late STCA alert due to tight parameters setting (success case)’, this event is implied in fault tree of OH 2 - 3 - 4 & 5. To determine safety requirements applicable to this event we had used a Top Down approach by deriving OH top level safety objective on different event which are composing fault tree.

3.4.3. Then, after derivation of top level OH safety objective, we had determined 4 different safety requirements applicable to EVENT 39 :

- For OH 2 safety requirement for Event 39 is equal to 1.14e-3 / flight hour
- For OH 3 safety requirement for Event 39 is equal to 2.7e-4 / flight hour
- For OH 4 safety requirement for Event 39 is equal to 4.48e-4 / flight hour
- For OH 5 safety requirement for Event 39 is equal to 9.65e-5 / flight hour

Safety requirements applicable to EVENT 39 is the most stringent value presenter here above then it is 9.65e-5 / flight hour

3.4.4. This study only addresses quantitative safety requirements due to time limitation constraints. No additional qualitative safety requirements (such as on procedures validation, training) were developed. Generally, safety requirements for human element take the form of training requirements for using a system or procedure.

3.4.5. In the following table, the most stringent value for each event (derived from OH1 and OH5) is presented and the derived safety requirement is defined in the third column.

3.4.6. As expressed in previous section, the value concerning an external event, an external failure or a human error was considered as an assumption to permit the determination of adapted safety requirement on the STCA system only and / or associated procedure(s). Indeed these values can not lead to safety requirements on STCA because they are not within STCA perimeter or because they concern human failure. The complete list of requirements and assumptions is presented in [REF 10] .

| Event Title | Stringent frequency value | Stringent Frequency Value Origin (OH) | Safety Requirements |
|---|---|---|---|
| Event 23 'Erroneous implementation of STCA parameter region' | 2.1e-4 / flight hour | OH 1 | The likelihood of an erroneous implementation of STCA parameter region **shall** be less than 2.1e-4 per flight hour. |
| Event 25 'SSR code / flight ID erroneously inserted in the suppression list of STCA' | 2.1e-4 / flight hour | OH 1 | The likelihood that a SSR code / flight ID is erroneously inserted in the suppression list of STCA **shall** be less than 2.1e-4 per flight hour. |
| Event 27 'Erroneous design of STCA algorithm' | 9.65e-5 / flight hour | OH5 | The likelihood of an erroneous implementation of STCA parameter region **shall** be less than 9.65e-5 per flight hour. |
| Event 37 'Late STCA alert due to erroneous parameters setting' | 9.65e-5 / flight hour | OH5 | The likelihood of a late STCA alert is issued due to erroneous parameters setting **shall** be less than 9.65e-5 per flight hour. |
| Event 39 'Late STCA alert due to tight parameters setting (success case)' | 9.65e-5 / flight hour | OH5 | The likelihood of a late STCA alert is issued due to tight parameters setting **shall** be less than 9.65e-5 per flight hour. |
| Event 43 'Error in implementation of STCA parameter region' | 9.65e-5 / flight hour | OH5 | The likelihood of an error in implementation of STCA parameter region **shall** be less than 9.65e-5 per flight hour. |
| Event 56 'Lack of STCA alert due to tight parameters setting' | 2.1e-4 / flight hour | OH 1 | The likelihood of an Lack of STCA alert due to tight parameters setting **shall** be less than 2.1e-4 per flight hour |
| STCA - LOSS 'STCA out of service' | 2.1e-4 / flight hour | OH 1 | The likelihood of having STCA out of service **shall** be less than 2.1e-4 per flight hour. |
| STCA - NUISANCE | 1.15e-3 / flight hour | OH 1 | The likelihood of an |

| Event Title | Stringent frequency value | Stringent Frequency Value Origin (OH) | Safety Requirements |
|---|---|---|---|
| 'Excessive nuisance STCA alert rate' | | | excessive nuisance STCA alert rate **shall** be less than 1.15e-3 per flight hour. |
| STCA - FALSE ' Excessive false STCA alert rate | 1.15e-3 / flight hour | OH 1 | The likelihood of an excessive false STCA alert rate **shall** be less than 1.15e-3 per flight hour. |

**Table 6 : Safety requirements to STCA system.**

3.4.7. The final likelihoods of the hazards (based on the most stringent values from table above) are presented in the next table and are compared against the safety objectives. Event values used to operate this complete fault tree computation are those one determined through safety requirements elaboration process. For each event, most stringent value had been determined as illustrated in 3.4.2 & in 3.4.3. After those values had been determined, they had been applied in all fault trees and computation had been performed to be sure that safety requirements determined ensure to met all top level safety objective determined for each OH.

3.4.8. After computation it is established that safety objectives are met for all hazards.

3.4.9. Note that only Option 1 (i.e. STCA with no option) for OH2 top event computation is represented below.

| Hazard title | Safety objective (per flight hour) | Top event result (per flight hour) |
|---|---|---|
| *OH1: Lack of ATCO instruction to solve a short-term conflict* | 8.3E-06 | 7.94E-06 |
| *OH2: Late ATCO instruction to solve a short-term conflict - no interaction with TCAS RA* | 4.5E-04 | 2.33E-04 |
| OH3: Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible | 7.2E-06 | 2.85E-06 |
| OH4: Avoiding instruction by ATCO received in en-route area simultaneously to a TCAS RA and incompatible | 8.8E-06 | 9.48E-07 |
| OH5: Avoiding instruction by ATCO received in TMA prior to a TCAS RA and incompatible | 3.8E-06 | 2.85E-06 |
| OH6: Avoiding instruction by ATCO received in TMA simultaneously to a TCAS RA and incompatible | 5.8E-06 | 9.48E-07 |

**Table 7: Fault Trees computation results**

# 4. Conclusion

4.1.1. Along the entire PASS project, safety-related work took a major place with the conduct of different activities. Firstly focused on operational hazards identification and risk assessment, the safety assessment process was focused in a second time on the determination of the (human and system) failure modes possibly leading to these operational hazards. Finally, the process permitted to elaborate generics requirements on the STCA system.

4.1.2. Operational hazards have been identified in two sequential steps. In a first step, basic operational hazards have been identified thanks to a strong collaboration between operational, technical and safety experts. This first operational hazard list has been refined in a second time to be more coherent with an agreed operational context and with some operational particularities. These two steps of operational hazard identification and refinement permitted to define consolidated event-trees and to apportion ATM safety targets on STCA-related operational hazards (without considering any involvement of TCAS as part of the mitigation means). It is important to note that it is one of the very first times that ATM safety targets have been apportioned on a safety-net like STCA (in accordance with the ESARR4 requirements for risk assessment in ATM).

4.1.3. Following operational hazards refinement and safety target allocation, a series of fault-trees has been created to permit the elaboration of safety requirements on the STCA system. To permit to only apportion requirements on the system it-self, hypotheses on human failures and on external event occurrence rates have been made and applied to all fault-trees. Following a top-down apportionment of the safety objectives on the fault-trees, safety requirements have been issued on different STCA failures. To permit this apportionment, a conservative approach has been taken that considered a basic STCA configuration which does not use any optional feature.

4.1.4. It is worth noting that the safety requirement concerning a particular failure which is involved in several fault-trees has issued from the most stringent failure frequency. Following this apportionment, it was also necessary to verify that the safety objectives defined during operational hazard analysis are met.

4.1.5. It is important to note that all derived safety requirements are generic ones and that they are based on hypotheses made on human failures, external event occurrences and on STCA configuration. To permit the elaboration of local safety requirements, which will correspond to specific ANSP needs, the whole process followed in this safety assessment would need to be customised with local ANSP input data.

# 5. References

[REF 1] 'PASS – Project Management Plan', EUROCONTROL, PASS/WA0/WP1/01/D version 1.1, 28th January 2008.

[REF 2] 'PASS - Consolidated analysis of a set of events of interest', EUROCONTROL, PASS_WA1_WP4_42W, version 1.1, 2nd December 2008

[REF 3] 'PASS - Analysis of SNET performance based on monitoring data', EUROCONTROL, PASS_WA1_WP5_64D, version 1.3, 29th April 2009

[REF 4] 'PASS - Descriptive analysis of observed SNET performance', PASS, PASS/WA1/WP4/90/W, version 1.0, 20/01/09

[REF 5] 'PASS - Preliminary Event Tree Analysis', EUROCONTROL, WA4/WP3/102/W, version 1.1, 20-10-2009

[REF 6] 'PASS – Performance metrics definition', EUROCONTROL, PASS_WA2_WP8_120D, version 1.0, 15th July 2009

[REF 7] 'PASS – Operational Safety Assessment Interim Report, EUROCONTROL, WA4/WP5/130/D, version 1.1, 24-02-2010

[REF 8] 'PASS – Consolidated List of Operational Hazards', EUROCONTROL, WA4/WP2/151W, version 0.2, 01-04-2010

[REF 9] 'PASS – Consolidated Event Trees Analysis, EUROCONTROL, WA4/WP2/152W, version 1.0, 24-06-2010

[REF 10] 'PASS – Preliminary Fault Trees Analysis, EUROCONTROL, WA4/WP2/155W, version 0.3, 30-07-2010

[REF 11] EUROCONTROL Specification for Short Term Conflict Alert, edition 1.1, 19/05/09

[REF 12] EUROCONTROL Safety Regulatory Requirement - ESARR2 Reporting and Assessment of Safety Occurrences in ATM, edition 2.0, 03-11-2000

[REF 13] EUROCONTROL, 2006, Air Navigation System Safety Assessment Methodology, Ed 2.1

[REF 14] EUROCONTROL Safety Regulatory Requirement - ESARR4 Risk assessment and Mitigation in ATM (2001)

[REF 15] EUROCONTROL Guidance Material for Short Term Conflict Alert. Appendix D-2: Functional Hazard Assessment of STCA for ATCC Semmerzake

[REF 16] EUROCONTROL Guidance Material for Short Term Conflict Alert. Appendix B-3: Outline Safety Case for STCA System

[REF 17] 'PASS - Preliminary Identification of STCA-TCAS Related Hazards', EUROCONTROL, WA4/WP1/91W, version 3.0, 17-04-2009

[REF 18] Final Report on post-RVSM ACAS full-system safety study, ASARP/WP6/58/D, version 1.0, 10/03/06

[REF 19] "EUROCONTROL Guidance Material for Short Term Conflict Alert- Appendix A: Reference STCA System", Edition 1.8, 11-08-2008

[REF 20] TCAS II performance in European TMAs - Part 1: Analysis Safety Issue Rectification Extension 2006-2008 Project - SIRE+ Project, Edition 1.1, 03rd February 2009.

[REF 21] ICAO, PANS-OPS Volume I, Part III, Section 3, Chapter 3.

[REF 22] Process for specifying risk classification scheme and deriving safety objectives in ATM, pending document

[REF 23] SRC Annual Safety Report 2009

[REF 24] SRC28.06, 15/03/07 ITEM 6.3

[REF 25] 'Human Factors Analysis of Safety Alerts In Air Traffic Control', Federal Aviation Administration, DOT/FAA/TC-07/22, November 2007

[REF 26] 'Main report for the: 2005/2012 integrated risk picture for Air Traffic Management in Europe', EEC Note No. 05/06, issued: April 2006

[REF 27] 'IAPA Study – Report on Safety Assessment Based on OSA Methodology', EUROCONTROL, IAPA/WP10/110D, version 1.5, October 2005

[REF 28] 'ACASA Work Package 1: Studies on the safety of ACAS II in Europe', EUROCONTROL, ACASA/WP1/210, version 1.3, March 2002

# ANNEX A: PROCESS FOR APPORTIONNING THE ATM SAFETY TARGETS

5.1. ESARR4 [REF 14] has established a Target Level of Safety for accidents (Severity Class SC1), 1.55E-08 flight.hour, which corresponds to the overall maximum frequency of accident whatever the type of accidents (e.g. mid air collision, controlled flight into terrain), directly caused by ATM for the ECAC area.

5.2. The European ED125 pending Document [REF 22] proposes a maximum tolerable frequency for the other severity classes. The Risk Classification Scheme (RCS) that sets the maximum ATM Safety Targets to be used as input to the project is presented in Table 8.

5.3. Note that this safety assessment is focused on current operations and not on future operations. Therefore no ambition factor has been considered to account for traffic growth.

| Severity Class | ATM Safety Target [flight hour] |
|---|---|
| 1 | 1.0E-08 |
| 2 | 1.0E-05 |
| 3 | 1.0E-04 |
| 4 | 1.0E-02 |

**Table 8: Safety Targets Based on ESARR4 Approach (ED125)**

5.4. The main accidents categories where ATM can make a significant contribution, either in causing or preventing accident, are:

- Mid-air collision
- Controlled flight into terrain (CFIT)
- Wake turbulence accident
- Runway collision
- Taxiway collision.

5.5. For the other accidents categories (loss of control in flight, take-off, landing, structural accident or fire/explosion), direct contribution of ATM is negligible.

5.6. The above categories are extracted from a EUROCONTROL document [REF 26] and are consistent with ESARR2 “Reporting and Assessment of Safety Occurrences in ATM” [REF 12] accident categories with the exception of the “wake turbulence” one, but this latter was considered to be of potential importance for ATM in that document [REF 26].

5.7. Two accident categories are applicable in the context of the PASS study. Indeed, the system under assessment (controllers assisted by STCA to prevent collision between aircraft) plays an important role in the prevention of mid-air and wake turbulence accidents.

5.8. In this EUROCONTROL document [REF 26], an analysis of historical accident rates was performed for each of these above accident categories. It is also assumed that ATC is the only element of ATM that contributes to the direct causes of accidents.

5.9. The contribution of ATC direct causes to each accident category that involved commercial flights in 2005 in the ECAC region is provided in the following table and is directly extracted from that report. It appears that these two accident categories, mid-air collision and wake turbulence accident, contribute to 33.52% of total accidents directly caused by ATC.

| | Fatal accident frequency per flight in 2005 | ATC Direct causes | Frequency of Fatal accident directly caused by ATC | % of fatal accidents directly caused by ATC |
|---|---|---|---|---|
| **Mid-air collision** | 5.40E-09 | 64.50% | 3.48E-09 | 31.46% |
| **Runway collision** | 3.30E-08 | 18.90% | 6.24E-09 | 56.34% |
| **Taxiway collision** | 3.40E-09 | 9.20% | 3.13E-10 | 2.83% |
| **CFIT** | 5.40E-08 | 1.50% | 8.10E-10 | 7.32% |
| **Wake turbulence accident** | 3.30E-09 | 6.90% | 2.28E-10 | 2.06% |
| **Loss of control in flight*** | 1.30E-07 | - | | |
| **Loss of control in take-off*** | 4.80E-08 | - | | |
| **Loss of control in landing*** | 6.40E-08 | - | | |
| **Structural accident** | 1.60E-08 | - | | |
| **Fire/explosion** | 2.20E-08 | - | | |
| **TOTAL** | 3.79E-07 | - | 1.11E-08 | 100.00% |

**Table 9: Contributions of ATC to Direct Causes of Fatal Aircraft Accidents for Commercial Flights within ECAC Region in 2005**

5.10. Potential ATM contributions to these accidents categories have not yet been estimated.

5.11. In this report it is assumed an average flight duration of 1.5 hour.

5.12. It is proposed to retain a more conservative value in the current analysis, viz. 30%, (in order to keep safety margins due to the uncertainties of statistical data handling) and to apply it to the total ATM TLS for all severity classes. The final TLSs corresponding to the retained risk budget that is used to derive safety objectives to “mid-air collision prevention” task by ATC assisted by STCA, are provided in the following table:

| Severity Class | Safety Target [flight hour] |
|---|---|
| 1 | 3.0E-09 |
| 2 | 3.0E-06 |
| 3 | 3.0E-05 |
| 4 | 3.0E-03 |

**Table 10: Apportioned Safety Targets**

# ANNEX B: Basic types of hazards

| Category | Basic Type of Hazard | Severity Class[4] |
|---|---|---|
| STCA vs. Conflict | Lack of genuine STCA alert | 3 |
| | Late STCA alert (i.e. below 20s before loss of separation) | 3 |
| | Delayed STCA alert (between 20s and 40s before a loss of separation) | 4 |
| | False STCA alert | 3/4 |
| | Nuisance STCA alert | 3/4 |
| ATC vs. STCA | Lack of ATC reaction to genuine STCA alert | 3 |
| | Late ATC reaction to genuine STCA alert | 4 |
| | Insufficient ATC reaction to genuine STCA alert | 3/4 |
| | Incorrect ATC reaction to genuine STCA alert | 3/4 |
| ATC vs. TCAS | TCAS RA and compatible ATC instruction simultaneously received by crew | 5 |
| | TCAS RA and contrary ATC instruction simultaneously received by crew | 4 |
| | Avoiding instruction by ATC contrary to subsequent TCAS RA | 4 |
| | Avoiding instruction by ATC contrary to ongoing TCAS RA | 3/4 |
| | Compatible instruction issued to a/c after TCAS RA report by crew | 5 |
| | Contrary instruction issued to a/c after TCAS RA report by crew | 3/4 |
| Crew vs. RA report | Lack of TCAS RA report by crew | 4/5 |
| | Late TCAS RA report by crew (40 seconds after TCAS RA) (after the clear of conflict) | 5 |
| STCA vs. TCAS | Time overlap between STCA alert and TCAS RA (*less than 15s before the TCAS RA activation)* | 4 |
| | STCA alert after TCAS RA | 3 |
| | STCA alert after Clear of Conflict advice by TCAS | 4 |

[4] N.B. Class 1 is the most severe; class 5 is the least severe.

# ANNEX C : EXAMPLE OF AN EVENT TREE ANALYSIS

5.13. This annex provides the event tree of hazard OH3: “Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible”.

## 5.14. Detailed Hazard Effects Analysis

5.14.1. The layout of the event tree is the following:

- The left-hand column shows the initiating event, i.e. the hazard in question.
- The second column from the right provides the consequences and the corresponding severity class of the various possible outcomes of the hazards.
- The intervening columns show the barriers that were identified as providing potential mitigation of the consequences of the hazard. The *Q* values show the probability that the related barrier would not be successful. The term “null” signifies that a barrier is not applicable in a given path.
- It is usual to show the mitigations in the order in which they are most likely to occur in order to aid understanding and help ensure that the logic is complete and correct.

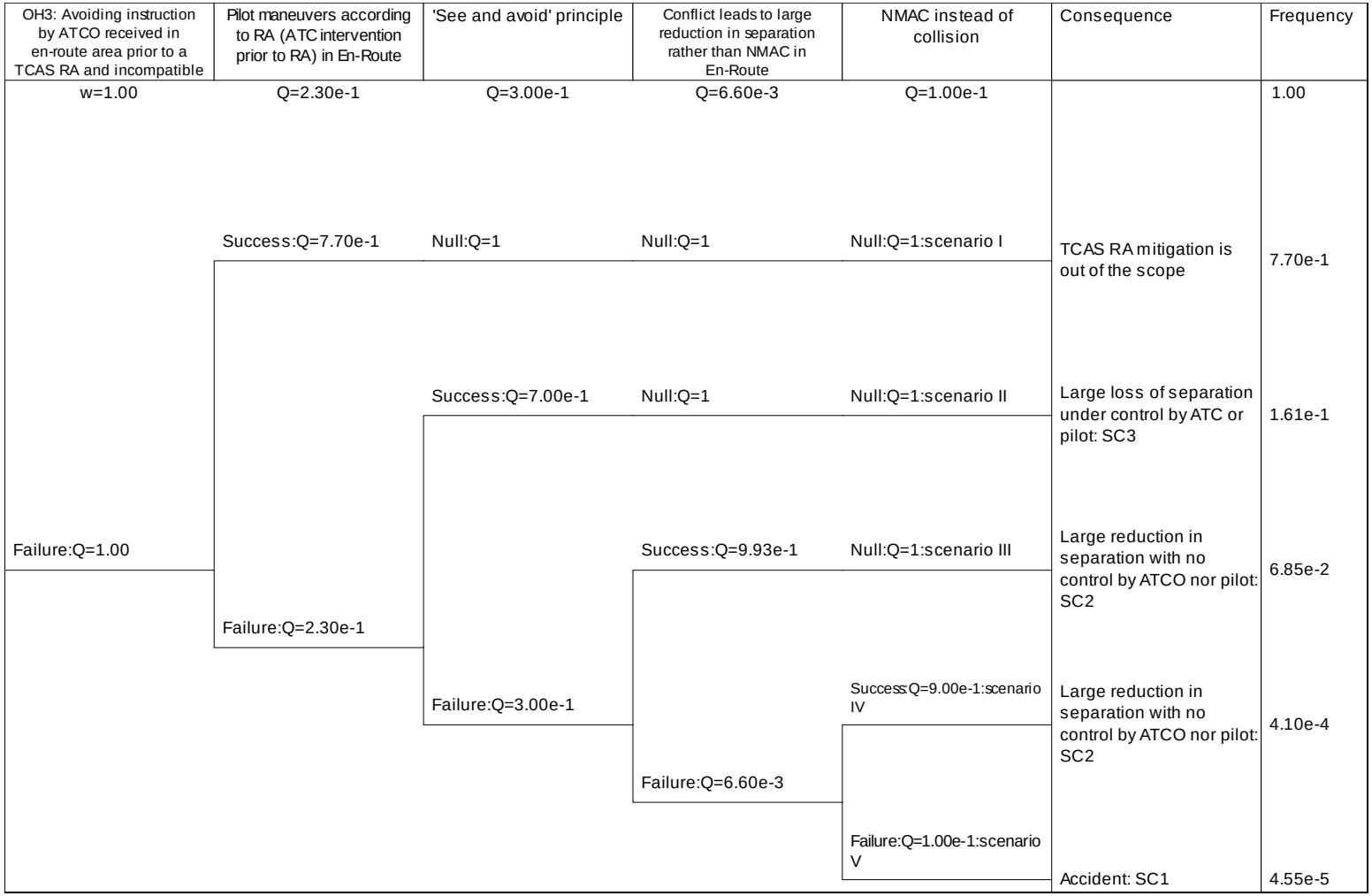



**Figure 5: Event Tree "Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible".**

5.14.1.1. Five possible effects scenarios have been identified after OH3.

5.14.1.2. In this hazard considered, the pilot who receives the avoiding instruction has time to start the manoeuvre but a few seconds later he/she receives a TCAS RA that is contrary to the avoiding instruction (*e.g.* an instruction to expedite climb is received when the RA requires a level-off). Because ATCO/STCA and TCAS are two independent loops the worst case is considered when the ATCO avoiding instruction and the TCAS RA are contradictory.

5.14.1.3. In the nominal sequence, in the event of an RA, pilots have to follow the TCAS RA even if there is a conflict between the RA and an ATC avoiding instruction to manoeuvre. Then this effect falls outside the scope of the Event Tree analysis and no ESARR4 severity class is assigned to this effect.

5.14.1.4. But experience shows that pilots do not always do this (see §5.3.7 of [REF 18]). The case where a small proportion of pilots may give precedence to a controller instruction over an RA is considered in the event tree.

5.14.1.5. Manoeuvres opposite to the sense of an RA might result in a reduction in vertical separation with the threat aircraft, especially when coordinated RA are triggered in both aircraft involved in the conflict. It might be ultimately mitigated by visual acquisition as the pilot is aware of the existence of a threat (see scenario II), the second barrier in the event tree. A severity 3 is assigned to that scenario.

5.14.1.6. If the “see and avoid” principle barrier fails and aircraft are close, it will not always lead to a collision. Indeed, some conflict configurations exist where the minimum distance between aircraft is more than 500 ft but less than 50% of separation minima. In such a case, the hazard effect is a large reduction in separation without crew and ATC controlling the situation. Therefore a severity of 2 is assigned to this scenario (cf. scenario III in the event tree above).

5.14.1.7. Finally it is generally reckoned that 10% of the cases, an NMAC could be a collision [REF 18] (severity 2, see scenario IV in case of NMAC and severity 1, see scenario V for the accident sequence - mid-air-collision or wake vortex accident).

5.14.2. Barriers Summary

5.14.2.1. The following table provides a summary of the barriers that have been identified as mitigating the effects of the hazard “Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible”.

5.14.2.2. The last column provides the probability of success of each barrier.

| Barrier | Description | Probability of success |
|---|---|---|
| Pilot manoeuvres according to RA (ATC intervention prior to RA) in En-Route | In the event of a RA, pilots shall follow the RA even if there is a conflict between the RA and an air traffic control (ATC) instruction to manoeuvre<br><br>*En-Route figure* | 0.77 |
| ”See and Avoid” principle | If visibility and conflict geometry permits, flight crew visually acquires the traffic aircraft proximity and thereafter takes appropriate action to avoid an NMAC or collision. | 0.70 |
| Conflict leads to large reduction in separation | This barrier deals with the conflict geometry. Given the environment, if there is a conflict that leads to larger reduction in separation it will not always lead to a near-mid air collision.<br><br>It means that the closest distance between aircraft will less than 50% of the separation minima but more than 500 ft.<br><br>*En-Route figure* | 0.993 |
| NMAC is not a collision | It is generally reckoned that 10% of the cases, an NMAC could be a collision. | 0.1 |

**Table 11: Barriers of “Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible” Hazard**

5.14.3. Safety Objectives Derivation

5.14.3.1. The safety objectives for each severity class are provided in next table, along with the Pe. Safety objectives for each severity class are defined based on the following formula:

$SO_i = \frac{ST_i}{Pe_i \times N_i}$, where Ni is equal to 6 (in TMA or in En-Route) as all identified hazards have credible effects in all severity classes.

| Severity | ST [per f.h] | Pe | SO [per f.h] |
|---|---|---|---|
| SC1 | 3.0E-09 | 4.6E-05 | 1.1E-05 |
| **SC2** | **3.0E-06** | **6.9E-02** | **7.2E-06** |
| SC3 | 3.0E-05 | 1.6E-01 | 3.1E-05 |
| SC4 | 3.0E-03 | | - |

**Table 12: Safety objectives for "Avoiding instruction by ATCO received in en route area prior to a TCAS RA and incompatible" hazard**

5.14.3.2. The most stringent safety objective is obtained from severity class 2.

# ANNEX D : EXAMPLE OF A FAULT TREE ANALYSIS

5.14.3.3. This annex provides the fault tree of hazard OH3: “Avoiding instruction by ATCO received in en-route area prior to a TCAS RA and incompatible”.

### 5.14.4. Causes Identification

5.14.4.1. Similarly to OH1, OH3 occurs because two aircraft are on a collision course (corresponds to a situation where ATCo is expected to issue an avoiding instruction and TCAS is expected to trigger corrective RA) combined with one of the following main causes:

- Either there is a late STCA alert;
- Or the controller reacts with delay to a genuine STCA alert;
- Or there is no STCA alert (same causes as for OH1) and the controller detects with delay the short term conflict.
- Or pilot react with delay to ATC avoiding instruction

5.14.4.2. Moreover the ATC avoiding instruction is incompatible with TCAS RA. This case has not been assessed and is not considered in the fault tree.

### 5.14.4.3. Causes leading to late ATCO Instruction to solve a short term conflict

5.14.4.3.1. The following causes associated to an erroneous design of STCA could lead to a late STCA alert:

- Inadequate design of STCA algorithm causing late alert;

5.14.4.3.2. As identified, an erroneous input to STCA can also lead to a late STCA alert:

- Error in implementation of STCA parameter region causing late alert;
- Late STCA alert due to inadequate parameters setting;
- Degradation of the surveillance inputs to STCA - late prediction of STCA;

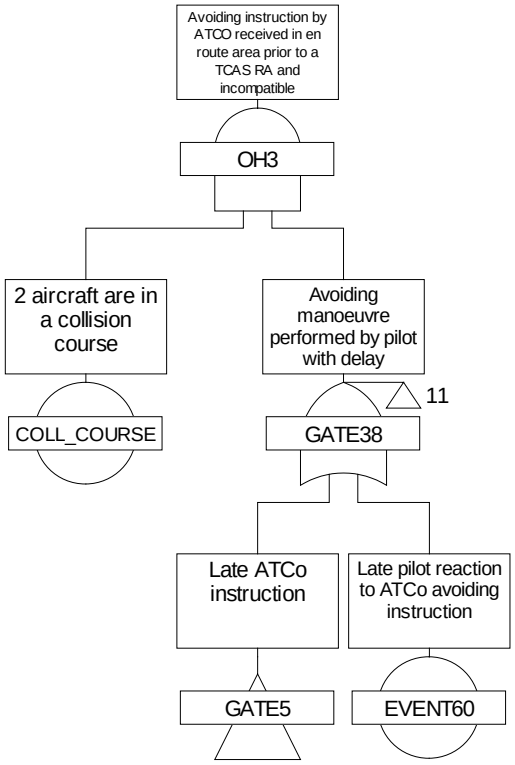
5.14.4.3.3. Moreover the cause “Late STCA alert due to tight parameters setting” encompasses the situations where STCA triggers late because of the tight tuning of its parameters in order to reduce the number of undesired STCA alerts (nuisance or false) that can lead to a loss of confidence by the controller with respect to the STCA system. According to WA2 feedback, STCA in nominal mode of operation alert will always trigger in case of severe conflict but may trigger late.

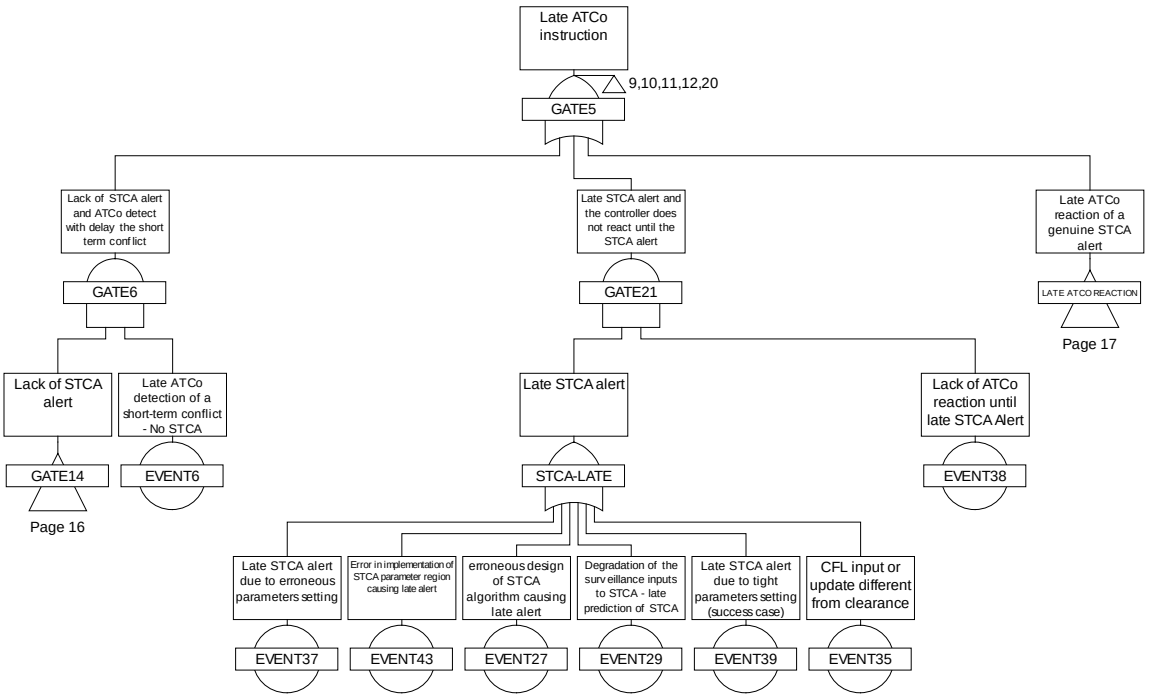
5.14.4.3.4. Other causes associated to problematic geometries can also affect the STCA alert timeframe:

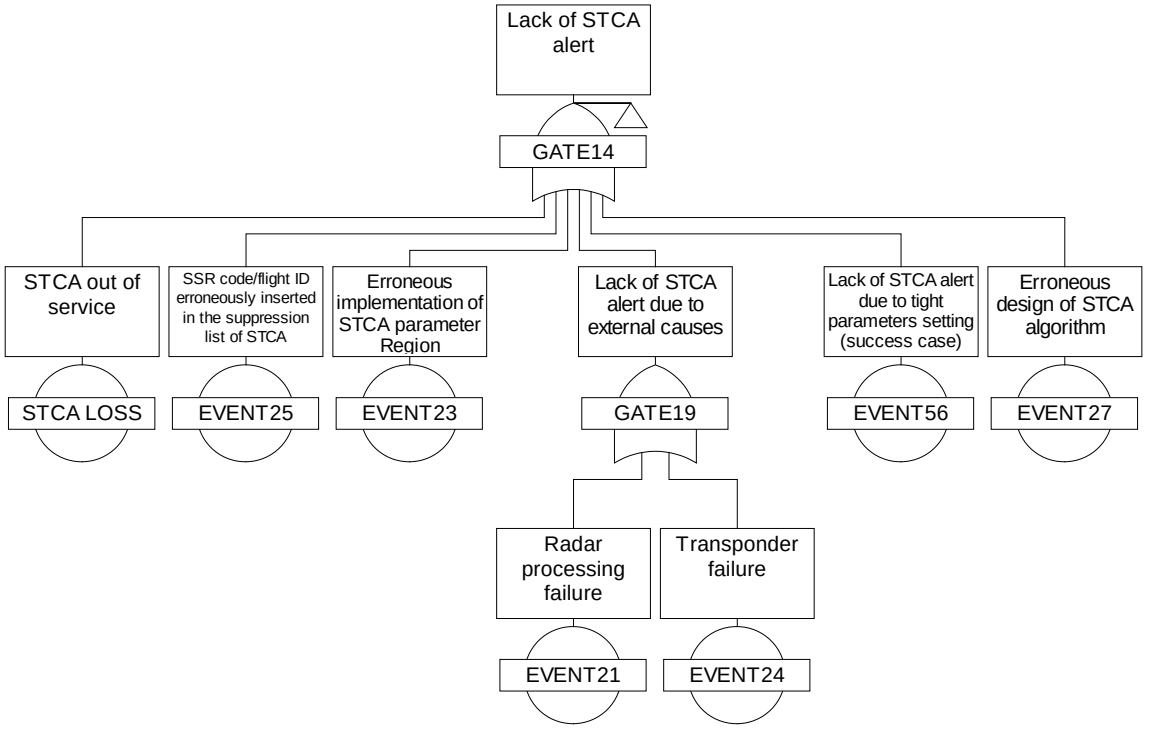
- Late STCA alert due to critical geometry in the vertical plane , or
- Late STCA alert due to critical geometry in the horizontal plane.

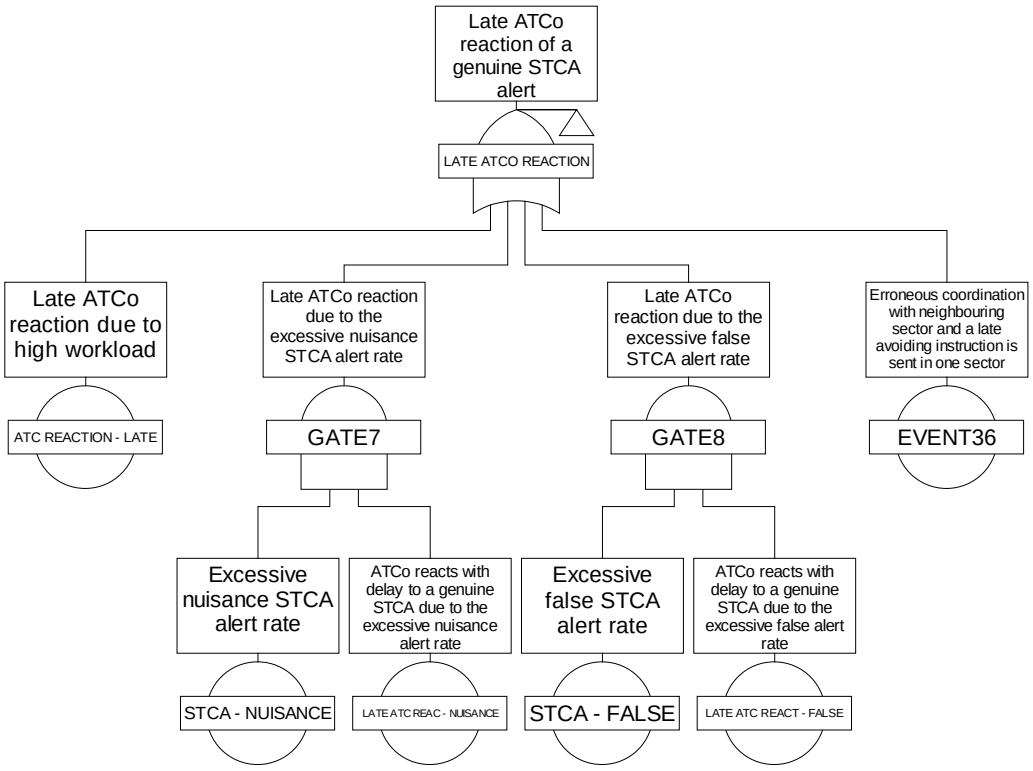
### 5.14.5. Fault tree Development of OH3

5.14.5.1. The next fault tree summarises the combinations of basic causes leading to the operational hazard.




Late ATCo instruction
9,10,11,12,20
GATE5
Lack of STCA alert and ATCo detect with delay the short term conflict
Late STCA alert and the controller does not react until the STCA alert
Late ATCo reaction of a genuine STCA alert
GATE6
GATE21
LATE ATCO REACTION
Page 17
Lack of STCA alert
Late ATCo detection of a short-term conflict - No STCA
Late STCA alert
Lack of ATCo reaction until late STCA Alert
GATE14
EVENT6
STCA-LATE
EVENT38
Page 16
Late STCA alert due to erroneous parameters setting
Error in implementation of STCA parameter region causing late alert
erroneous design of STCA algorithm causing late alert
Degradation of the surveillance inputs to STCA - late prediction of STCA
Late STCA alert due to tight parameters setting (success case)
CFL input or update different from clearance
EVENT37
EVENT43
EVENT27
EVENT29
EVENT39
EVENT35


Lack of STCA alert
GATE14
STCA out of service
SSR code/flight ID erroneously inserted in the suppression list of STCA
Erroneous implementation of STCA parameter Region
Lack of STCA alert due to external causes
Lack of STCA alert due to tight parameters setting (success case)
Erroneous design of STCA algorithm
STCA LOSS
EVENT25
EVENT23
GATE19
EVENT56
EVENT27
Radar processing failure
Transponder failure
EVENT21
EVENT24




### 5.14.6. Basic Causes Probability Determination for OH3

5.14.6.1. The next step in the fault tree analysis consists in apportioning the safety objective to the different causes of a given hazard. This allocation is performed 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.
- A bottom-up allocation process: it consists in assigning a probability to each basic event based on engineering judgement.

5.14.6.2. The total frequency of events in which there is a late ATCO reaction is determined by the number of late ATCO reaction over the total number of flight hours. According to paper 91 [REF 17], 3.4.4, page 14, a late ATCO reaction to STCA is defined as a reaction occurring more than 30 seconds after the STCA alert has gone off. From paper 64, 3.3.4.1 page 34 [REF 3], it is possible to calculate that the ATCo reaction to STCA occurring after 29 seconds (i.e. late) are 22. In this way it is possible to calculate that the event frequency of a late ATCO reaction is 22 / 8391995,33 = 2,622e-6 / flight hour

5.14.6.3. Find hereafter an illustration of safety objective apportionment on two basic events.

| Event Reference | Frequency (Flight Hour) | Rationale |
|---|---|---|
| **OH3 Avoiding instruction by ATCo received in en route area prior to a TCAS RA and incompatible** | | |
| Event 60: “Late pilot reaction to ATCO avoiding instruction” | 2,264e-6 / flight hour<br><br>**5.75e-4 / flight hour** | Ref. paper 64 [REF 3] 3.4.2.3. page 38 “Two sets of reactions seem to exist: timely reactions distributed along a curve up to 25 seconds and, based on limited data, late reactions distributed uniformly after that. In the first set, the use of avoiding instruction phraseology allows an average gain of 3 seconds on the implementation of the manoeuvre, i.e. from 11.7 seconds to 8.6 seconds.”<br><br>Value was calculated this way: total late reactions (i.e. after 25 sec.)/ total hours flight in the core area = 19/8391995,33= 2,264e-6 / flight hour<br><br>Frequency presented here above is based on a statistical study. During the allocation process a more conservative (pessimistic) value was preferred, which is presented in red in the “frequency” column. |
| COLL_COURSE ‘2 aircraft are on collision course | 3.3e-3 / flight hour | Value taken as a conservative hypothesis. Following several STCA configuration test, it appears that the more stringent alert frequency is equal to 3.3e-2. We estimate that 10 percent of this frequency is a representative estimation to evaluate numbers of A/C which are on collision course and which are not detected by STCA. |
| | | |
| **Gate 5 Late ATCo instruction** | | |
| Event 6 “Late ATCo detection of a short term conflict - No STCA | 1.65e-2 / flight hour | Value determined thanks to a top down approach applied to fault trees.<br><br>During the allocation process a conservative (pessimistic) value was preferred |

| | | |
|---|---|---|
| Event 27 ‘Erroneous design of STCA algorithm’ | 2.7e-4 / flight hour | Value determined thanks to a top down approach applied to fault trees. |
| Event 29 ’Degradation of the surveillance inputs to STCA - late prediction of STCA | 2.7e-4 / flight hour | Value determined thanks to a top down approach applied to fault trees. |
| Event 35 ‘CFL input or update different from clearance’ | 2.7e-4 / flight hour | Value determined thanks to a top down approach applied to fault trees. |
| Event 37 ‘Late STCA alert due to erroneous parameters setting’ | 2.7e-4 / flight hour | Value determined thanks to a top down approach applied to fault trees. |

**Table 13: Example of Safety objectives apportionment through fault trees**

*** END OF DOCUMENT ***