EUROCONTROL

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

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

EUROCONTROL

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidance Material for Short Term Conflict Alert **Appendix D-2: Functional Hazard Assessment of STCA for ATCC Semmerzake**		
Document Identifier	**Edition Number:**	2.0
EUROCONTROL-GUID-123	**Edition Date:**	19 May 2009

Abstract

This document describes the analysis of STCA for ATCC Semmerzake. The specific military environment (military formation flights and a large number of primary tracks) creates a large number of nuisance alerts. This document describes the Functional Hazard Assessment of a number of specific solutions to try to reduce the nuisance alert rate.

Keywords

Safety Nets
STCA

Contact Person(s)	Tel	Unit
Ben Bakker	+32 2 72 91346	CND/COE/AT/AO

STATUS, AUDIENCE AND ACCESSIBILITY

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

ELECTRONIC SOURCE

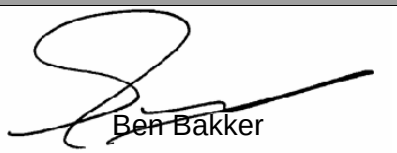
Path:	\\HHBRUNA02\bakkerb$\QC	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	455 Kb

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

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

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Technical Manager	 Ben Bakker	19-5-2009
Head of ATC Operations and Systems Unit	 Martin Griffin	19-5-2009
Deputy Director Network Development	 Alex Hendriks	19-5-2009

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
1.0	14-12-2006	Template	All
2.0	19-5-2009	Alignment with updated EUROCONTROL Specification for STCA	Front matter only

CONTENTS

FOREWORD

ATCC Semmerzake is the Belgian Military ATC Unit. It is equipped with a modern ATC system that contains amongst others an STCA application. However, the specific military environment (military formation flights and a large number of primary tracks) creates a large number of nuisance alerts, rendering STCA ineffective.

In the period May 2006 to September 2006, ATCC Semmerzake and EUROCONTROL, supported by QinetiQ and Deep Blue, collaborated to develop specific solutions to reduce the nuisance alert rate.

This document is one of a set of two documents that describe the actions undertaken and the results achieved. The document set includes:

- Optimisation of STCA for ATCC Semmerzake
- Functional Hazard Analysis (FHA) of STCA for ATCC Semmerzake [This document]

The document set forms a Case Study in applying the optimisation and safety assurance guidance material that supports the EUROCONTROL Specification for STCA, and as such is guidance material in its own right.

Note however that the developed specific solutions should not be adopted without performing similar analyses to determine the applicability in the target environment.

1. INTRODUCTION

1.1 Overview of the study

The STCA system installed at ATCC Semmerzake (where Belgian military ATC is in operation) suffers from a number of known problems that severely restricts its usability, and with the result that most of the time STCA remains switched off at the controller working position. As a matter of fact military aircraft perform manoeuvres that civil aircraft do not, such as flying in formation, flying in radar trail, dog-fighting and executing very fast turns. This style of flying results in a large number of unwanted STCA alerts and generates an increased workload for controllers, through assessing alerts for validity.

These problems are described and analyzed in detail in the companion document being part of the present case study: “Appendix D-1: Optimisation of STCA for ATCC Semmerzake”. The document presents specific technical solutions to overcome the identified problems and make the STCA system usable in Belgian Military Airspace.

While the present document is aimed at explaining the process and at documenting the results of a Functional Hazards Assessment (FHA) Workshop performed at ATCC Semmerzake once the new technical solutions for STCA were identified. The results include the list of hazards identified during the workshop, an estimation of their severity and a few examples of mitigation means proposed by workshop attendees to mitigate the hazards which were perceived as more severe.

Section 2 illustrates the motivations of the FHA Workshop and the method adopted to perform it. Section 3 describes the operational scenarios used as input to the discussion during the FHA. Section 4 presents the checklist which was adopted to support hazard identification through the analysis of operational scenarios. Section 5 describes how the workshop has been organized.

Finally section 6 present a record of the results achieved with the Functional Hazards Assessment of ATCC Semmerzake STCA, with a few conclusions derived in section 7.

2. THE FHA WORKSHOP

2.1 Aim of the workshop

The FHA workshop was organized involving participants with a wide variety of experience and knowledge related to the STCA, including operational, technical and safety experts. As anticipated above, it aimed at performing a first safety assessment of ATCC Semmerzake STCA, taking into account the new technical solutions previously identified and documented in "Appendix D-1: Optimisation of STCA for ATCC Semmerzake".

The workshop was performed in two days and was organized following the recommendations of the Safety Assessment Methodology of EUROCONTROL. When applicable, it was compliant with the ESARR 4 requirements, to serve as a prerequisite for an overall safety assessment study of the STCA system.

More specifically the workshop was addressed at identifying and discussing about the following safety issues:

- The **hazards** potentially causing a lack of safety benefits (i.e. **safety not enhanced**) with respect to the full potential benefit of STCA.
- The **hazards** potentially determining a **negative effect on safety** as opposed to the operational condition without STCA
- The potential **effects** of the hazards identified on Air Traffic Management systems and activity.
- The **estimated severity** of the hazards identified
- The identification of possible **mitigation means** to prevent the identified hazards and to mitigate their consequences.

Due to the limited time available and to the guidance purposes of the case study, it was decided to limit the scope of the workshop to the issues listed above. Thus the overall activity did not include an estimation of hazard frequency and a definition of safety objectives, as a typical FHA should normally encompass.

Note that controllers at ATCC Semmerzake are – in most of the cases – not using the currently available STCA. Thus ***the system under assessment was in practice the whole STCA including the new technical solutions***. However, the workshop was organized in such a way that most of the attention was focussed on the new technical solutions, to assure at the same time an appropriate understanding of the safety implications of the new solutions and a concrete operational feedback, aimed at a further refinement of the system specifications related to the new solutions.

2.2 Technical solutions under analysis

The new technical solutions proposed to improve STCA in the Belgian military environment and to make it usable are documented in detail in the companion document named “Appendix D-1: Optimisation of STCA for ATCC Semmerzake”. The following sections will assume a sufficient understanding of that document by the reader and will not describe specifically the new algorithms and parameters included in the optimization study. However, for the sake of clarity, the new proposed solutions are briefly summarized in the table below.

New Technical Solutions		***Objective***
1	Split track detection logic	*Minimize false alerts caused by split track phenomena*
2	Military formation detection logic	*Minimize nuisance alerts caused by aircraft operating in formation*
3	Reduction of look ahead time from 5 to 2 minutes	*Minimize nuisance alerts related to linear prediction limitations*
4	Region dependent parameters in 10 parameter groups	*Minimize nuisance alerts, taking into account the different operational constraints of various areas of airspace and the variety of aircraft potentially in conflict*
5	VFR SSR codes with maximum assumed flight level	*Minimize unwanted alerts triggered by VFR tracks, which may be safely assumed to be at low level.*
6	List of training SSR codes for each aerobatic area	*Eliminate unwanted alerts caused by training exercises in aerobatic areas*
7	Assignment to wingmen of leader’s vertical state (Z, VZ)	*Minimize nuisance alerts related to wingmen operating in formation, by allowing STCA to test in the vertical dimension.*

2.3 Selection of participants

A typical FHA session needs to involve representatives of all the main stakeholders concerned with the system under analysis and with the consideration of its safety.

The FHA organised in Semmerzake involved the following roles:

- ***System users***: four senior controllers and members of the Belgian air staff, to identify and assess the consequences of hazards from an operational perspective;
- ***System technical experts***: one technical expert from the Belgian ATCC to explain the system purpose, interfaces and functions;
- ***Safety experts with operational background***: three safety experts from the Belgian Aviation Safety Directorate and the ATCC to bring wider experience of the effects of hazards;
- A ***Safety expert with methodological background*** from Deep Blue to guide in the application of the FHA methodology itself;
- A ***Validation expert*** from EUROCONTROL to ensure adequate links between the FHA activity and the other validation activities of the SPIN task force;
- A ***Facilitator*** (from Deep Blue) to lead the session and guide the meeting through the different steps of the FHA process.
- A ***Meeting Secretary*** (from QinetiQ), to record and summarise the findings, and assist the facilitator in ensuring that all technical and operational aspects have been covered.

2.4 Available methods for FHA facilitation

As suggested in the Safety Assessment Methodology both functional and creative thinking are necessary during FHA workshops to ensure that the identification of potential hazards is as comprehensive as possible *[Ref: Eurocontrol SAM FHA Guidance Material: FHA Chap 3 Guidance Material B1 (Identification of Failure Modes, External Events and Hazards) and Guidance Material B2 (Identification of Hazards)]*. It is important to encourage participants to think widely and imaginatively around the subject, initially without analysis or criticism. On the other hand, while group sessions are usually good at generating ideas, identifying issues and making an initial assessment, they do not always produce these outputs in a logical order. Also, it is difficult for a group to analyse the ideas and issues in detail – it is hard to consider all the implications and inter-relationships between issues when these have only just been raised. Much time can be wasted in highly technical discussions which may turn out to be irrelevant. Thus FHA workshops need to use well defined and structured techniques. The technique adopted should

both ensure completeness and encourage (not constrain) wide-ranging thinking about the system.

Several techniques are available for this purpose. We considered three of them as particularly adequate:

- HAZOP (HAZard and OPerability study);
- Tracer Lite
- Scenario guided (what-if) interview.

2.4.1 HAZOP

Hazop aims at discovering potential hazards, operability problems and potential deviations from intended operation conditions. It supports establishment of approximate likelihood and identify consequence of events. It is based on a group review, and it is structured on specific guidewords, based on a representation of the system to be produced in advance as input. HAZOP considers the various aspects of the operation analysing the flow of the activity and the possible deviations from the expected behaviour, prompted by guidewords. HAZOP has been developed in the chemical domain but in recent years it has been widely accepted within other sectors, including ATM. HAZOP can rapidly spot those functionalities whose failure mode effects can be remedied. It recognises existing safeguards and develops recommendations for additional ones.

2.4.2 Tracer Lite

Trace Lite has been specifically developed to predict human errors that can occur in ATM systems, considering the procedural, equipment, and organisational framework in which humans operate. It builds on error models in other fields, integrated with considerations about information processing in ATM. Tracer Lite requires as input a task analysis of the process of using the ATM system, focussed on the most critical tasks (in order to limit the complexity of the analysis). Tracer Lite can be used for both retrospective and predictive studies, it is less consolidated then HAZOP, however it has been used by EUROCONTROL in several ATM projects including the Conflict Resolution Assistant and the Mediterranean Free Flight projects.

2.4.3 Scenario guided (what-if) interview

The Scenario Guided (what-if) interview is the more consolidated and intuitive of the techniques considered. It requires some representative scenarios of usage for the concept or tool under study. Operational experts are guided through the scenarios and interviewed with a "what if" approach. This is a technique particularly appreciated by operational experts as it is very close to the operational environment. However, the analysts have to pay particular attention in the scenarios selection, as the achievable results are likely to be

very specific. In addition, the results need to be extrapolated and generalised, to integrate them with other information such as those available to the operational and technical experts of the system under analysis.

2.5 The selected method: Scenario guided (what-if) interview

The ease of use and the strict schedule for the preparation of the workshop led to the selection of the *Scenario guided, what-if interview*.

A set of 7 operationally relevant scenarios was identified, in collaboration with Belgian military ACC representatives in the SPIN task force. As anticipated before, the scenarios aimed to address specific military issues which have an impact on STCA functioning and to focus the discussion on possible hazards related to the new technical solutions.

1. Flight in formation/trail

2. Area to airway

3. Area to Area

4. STCA inside an Area

5. VFR/Unknown Traffic

6. Authorized penetration

7. Crossing airways

When starting the FHA, each scenario was presented to workshop attendees in a tabular format, including four different categories of information:

- Description of the scenario
- Operational implications
- STCA implications
- Technical solutions adopted in the enhanced STCA

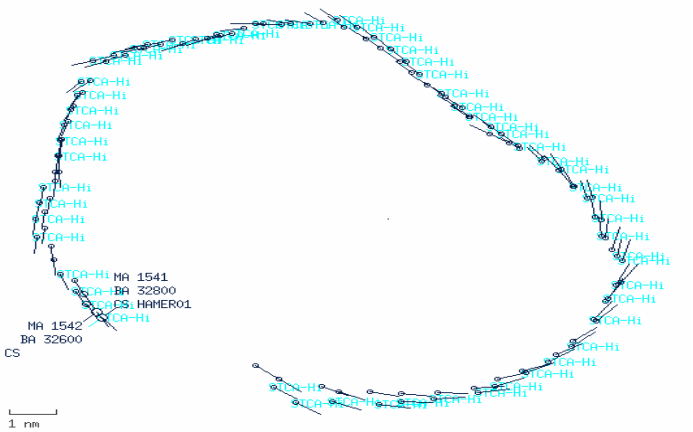
In some cases a picture taken from the “Appendix D-1: Optimisation of STCA for ATCC Semmerzake” was also added, allowing a better understanding of the situation, based on examples of typical traffic situations specific for the scenario.

The following section presents each scenario in a tabular format similar to the one used during the workshop.

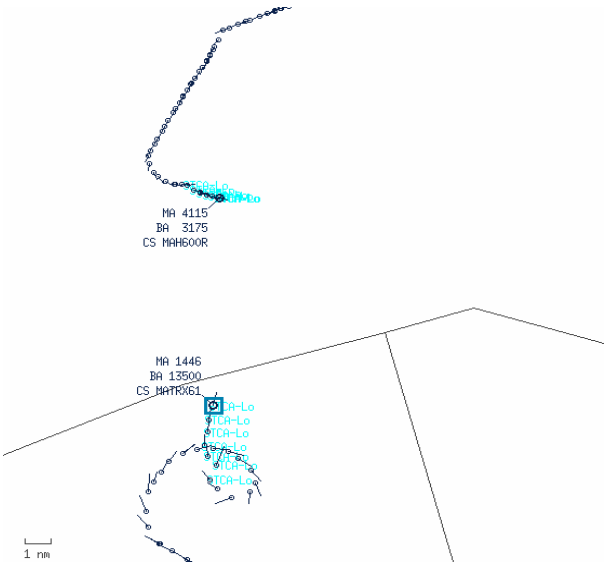
(Intentionally blank)

3. SELECTED SCENARIOS

3.1 Flight in formation/trail

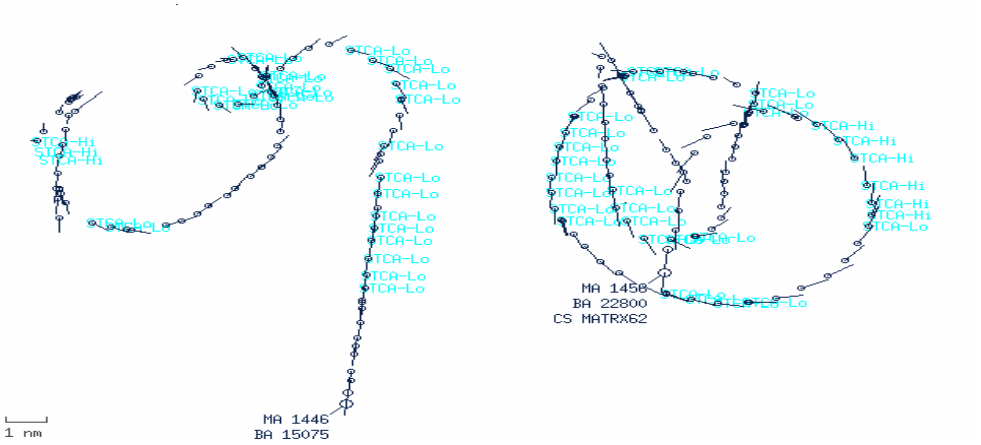
OS 1 - FLIGHT IN FORMATION/TRAIL	
Description	**Military aircraft performing the following procedures:** **1) Radar Trail** **2) Join Up** **3) Formation Flying** **4) Split Formation**
Operational implications	▪ *Radar Trail* Only the first and the last squawking in the trail 2 miles maximum distance between 2 aircraft Typical for take off and recovery in bad weather conditions. ▪ *Join Up* Continuous alerts are generated while joining Wingmen stop squawking Mode A and C once joined up. ▪ Formation Flying Only the leader is transponding Mode A and Mode C. All Aircraft are assumed to be on the same flight level. ▪ *Split Formation* Wingmen will start to squawk A and C when instructed by ATC. Once identified, the wingman is split from the rest of the formation.
STCA implications	▪ Undesirable to have STCA alert between a/c joined in formation flight. ▪ As the lateral separation is less than 5 NM, continuous alerts are generated amongst elements of the formation/trail. These alerts are considered nuisance alerts cluttering potential real alerts.
Example Picture 	
Technical solution adopted in the new STCA	▪ ***Formation flight logic to prevent unwanted alerts when the formation flight is recognized.***

3.2 Area to Airway

OS 2 - AREA TO AIRWAY	
Description	**Traffic manoeuvring inside a military area next to a civil airway (ATS routes) with lateral or vertical manoeuvres.**
Operational implications	▪ Short reaction time for controllers to react if A/C penetrates civilian airspace. ▪ High speed manoeuvring, high ROC/ROD and steep turns versus steady flight profile. ▪ Aerobatics being performed both by singletons and by formation flights. ▪ Need for ATCOs to input BFL (Block Flight Levels).
STCA implications	▪ Nuisance alerts are generated inside formations. ▪ Nuisance alerts due to excessive prediction times and high speed manoeuvring. ▪ BFL to be taken into account at the CWP ▪ Linear (any) prediction less accurate for the military traffic. ▪ If aerobatics are performed in formation, split tracks can occur.
Example Picture 	
Technical solution adopted in the new STCA	▪ ***Creation of buffer zones around aerobatic areas using wider parameters as the Aircraft approaches the boundaries of the area[1].*** ▪ ***Use of BFL as in the current system.*** ▪ ***Dynamic activation/de-activation of STCA regions (improved FUA Level3).***

[1] Note that in the proposed enhancement of the system all prediction times were anyhow restricted to less than 2 minutes. While in the original STCA they arrived even to a maximum of 5 minutes.

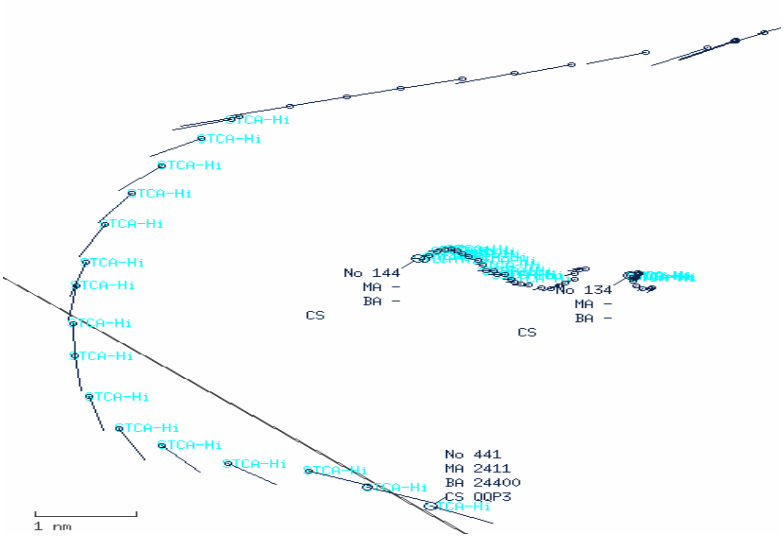
3.3 Area to area

OS 3 - AREA TO AREA	
Description	**Two military flights manoeuvring inside neighbouring area with lateral or vertical manoeuvres.**
Operational implications	▪ Shorter reaction time for controllers to react if A/C tends to penetrate civilian airspace. ▪ High speed manoeuvring, high ROC/ROD and steep turns versus another aircraft with high speed manoeuvring, high ROC/ROD and steep turns. ▪ Aerobatics may be performed by singletons as well as by formation flights. ▪ BFL needs to be input.
STCA implications	▪ Nuisance alerts due to excessive prediction times and high speed manoeuvring. ▪ BFL is taken into account at the CWP. ▪ Limited available warning time. ▪ Linear prediction less accurate for manoeuvring tracks. ▪ If aerobatics are performed by a formation, split tracks can occur.
Example Picture 	
Technical solution adopted in the new STCA	▪ ***Creation of buffer zones around aerobatic areas using wider parameters as the aircraft approaches the boundaries of the area.*** ▪ ***Use of BFL as in the current system.*** ▪ ***Dynamic activation/deactivation of STCA regions (improved FUA Level3).***

3.4 STCA inside an area

	OS 4 - STCA INSIDE AN AREA
Description	**Aircraft participating in an exercise inside the same geographical area.**
Operational implications	▪ Aircraft are widely dispersed over a certain area but operating together. ▪ Aircraft intentionally manoeuvre towards each other. ▪ Aircraft are squawking individually.
STCA implications	▪ Nuisance alerts are generated as the aircraft are manoeuvring towards each other.
Technical solution adopted in the new STCA	▪ ***List of "training mode A codes specified off line for each area.*** ▪ ***List of "training" Mode A codes assigned to aircraft participating in exercises in the specific area.*** ▪ ***Suppression of alerts between aircraft squawking a relevant training code.***

3.5 VFR versus unknown traffic

OS 5 - VFR/UNKOWN TRAFFIC	
Description	**Penetration of active working areas by:** **1) Primary tracks** **2) Tracks with Mode A without Mode C** **3) Tracks with Mode A and C**
Operational implications	▪ Aerobatics may be performed by singletons as well as by formation flights. ▪ Unlike neighbouring countries, controlled airspace in the BE FIR/UIR starts from 4500 ft AMSL. VFR flights entering the country should be flying below 4500 ft AMSL, but it occurs that VFR flights enter controlled Class C airspace.
STCA implications	▪ If no Mode C is present, the track is assumed to be flying at any possible level and processed 2-dimensionally. ▪ Although these flights are assumed to operate below the controlled airspace, nuisance alerts generated against VFR / unknown traffic.(primary ; Mode A without valid C).
Example Picture 	
Technical solution adopted in the new STCA	▪ ***Construction of a Mode A code list, specifying the minimum and maximum assumed flight level of slow moving aircraft, with various VFR mode A codes that have no mode C.*** ▪ ***Construction of a volume from 0 to 4500ft covering the whole area of interest in which much narrower parameters (3NM and 45 seconds) are applied.***

3.6 Authorized penetration

OS 6 - AUTHORIZED PENETRATION	
Description	**Authorized penetration in military Area:** **1) transit of a Mil aircraft through an active TRA** **2) transit of civil aircraft (eg, approved direct routing, FUA Level3, etc.).**
Operational implications	▪ CFL/BFL must be input. ▪ Restrictions may be imposed on the Operational Air Traffic. ▪ Transit Traffic has steady flight Profile. ▪ Can be considered as for FUA Level 3 (GAT crossing above our Airspace).
STCA implications	▪ CFL/BFL must be used. ▪ STCA will be generated if required.
Technical solution adopted in the new STCA	▪ ***STCA generated based on the parameters of the area (e.g. less than 5NM separation)***

3.7 Crossing airways

0S 7 - CROSSING AIRWAYS	
Description	**Military traffic crossing ATS route.**
Operational implications	▪ Steady profiles (steady course and level). ▪ Generally done after coordination with the civil ATS. ▪ Military are responsible for separation if not coordinated.
STCA implications	▪ More warning time available. ▪ Linear prediction accurate enough. ▪ Use of CFL. ▪ If coordinated, no STCA alerts should be generated.
Technical solution adopted in the new STCA	▪ ***Military formation and Split Track logic.*** ▪ ***Creation of STCA Area with wider parameters (using the buffer zone).*** ▪ ***STCA parameters set to same or similar values to Civil STCA parameters.***

4. CHECKLIST OF 'KEYWORDS' AND 'PROMPTS'

In addition to the use of scenarios, the method adopted can also rely on the use of a checklist of 'prompts' or 'keywords' to help workshop participants to think about possible hazards, related to the system under analysis. During the workshop at ATCC Semmerzake the attendees were provided with the checklist shown in Table 2. It is an adaptation of the checklist illustrated in the SAM Methodology *[Ref: Eurocontrol SAM FHA Guidance Material: FHA Chap 3 Guidance Material B1 (Identification of Failure Modes, External Events and Hazards)]*.

ATM EQUIPMENT COMPONENT	**OPERATOR**
STCA	Controller
Other components or functions related to the STCA (e.g. Transponder, CWP HMI, CFLs, etc).	Pilot
	Other operators (whose actions affect the STCA functioning)

FAILURE MODE (equipment component)	**FAILURE MODE (operator)**
Total loss	Omitted operation
Partial loss	Delayed operation (too late)
Erroneous updating	Premature operation (too early)
Erroneous setting	Inadvertent operation
Error of input/ output:	Modified operation
- missing data (partial loss, total loss)	Violation of operation (Routine or unintentional)
- detected erroneous/corrupted data (not credible error/corruption)	Used beyond intent
- undetected erroneous/corrupted data (credible error/corruption)	Misunderstood
- out of sequence	Misheard
- out of range	Failure to start/stop
	Failure to switch

Table1: the checklist for the *what if interview* session

It is to be noted that –consistent with the SAM Methodology approach – the checklist suggests two main drivers for a failure mode or a hazard to happen: namely technical failures at the level of ATM equipment components and operational failures of roles involved in the activity supported by the system under assessment. However, not mentioned in the checklist, FHA participants are also encouraged to think about *external events* (e.g. severe weather phenomena) which can contribute to a failure condition or hazard.

5. ORGANISATION OF THE WORKSHOP

The workshop was organized based on the following phases:

1. Introduction and description of the system
2. Identification of hazards
3. Classification of hazards by severity
4. Identification of mitigation means
5. Consolidation

The following sections provide a very quick description of the methodological process, as it was specifically deployed during the workshop. The reader who is only interested in the documentation of FHA results should skip to section 6.

5.1 Introduction and description of the system

The first phase was devoted to presenting the aim, methods and expected results of the FHA and to ensure a common understanding of workshop objectives.

Considerable time was spent to present the main characteristics of the system under investigation. In particular, a basic explanation of the STCA functioning was provided for those who were not very familiar with safety nets. Then a specific presentation focussed on the new technical solutions identified to enhance the previously existing STCA.

5.2 Identification of hazards

The second phase was divided in 3 steps:

a) Explaining the method

At this stage people were instructed on the basic rules for taking part in the discussion (e.g. being open-minded, don't dominate the discussion, let everyone express his position, avoid having a "protective" attitude towards the system under study and towards operational people, etc.).

Then people were familiarized with the structure of the table describing the scenarios and about the possibility to use the checklist as a support for generating ideas.

b) Describing a specific operational scenario

Once participants were familiarized with the method, a specific scenario was analyzed in detail, allowing everyone read individually the scenario for a few minutes and then providing clarifications when needed.

c) *Brainstorming session (for hazard identification)*

After a specific scenario was analyzed in sufficient detail, the brainstorming session began, allowing all participants propose ideas about possible hazards. As the number of people taking part in a brainstorming should normally not exceed 6-7 people, it was decided to split the participants in 2 subgroups. Each group had its own facilitator, who had the responsibility for taking notes of the ideas generated by the group for about 30 minutes. At the end of each brainstorming session the two groups joined up to present the identified hazards in the plenary session. The facilitator and the secretary had the responsibility to make a unified list of hazards, distinguishing the hazards identified by both groups and the ones proposed by only one group.

The steps ‘b’ and ‘c’ were repeated for each scenario, to let the brainstorming start just after the familiarization by people with a specific scenario. It is to be noted that scenarios were used as a support to the generation of hazards and not as constrain to limit the discussion. If a participant proposed a hazard not relevant for the scenario under discussion, the secretary took note of it for further discussion during the following phases of brainstorming.

Due to the strict time constraints (one day of workshop available for the identification of hazards) only 4 out of 7 scenarios were addressed. Despite this limitation, the number of hazards identified was anyhow relevant and probably covering also part of the following scenarios. This can be credibly assumed as the more the analysis of scenarios progressed the more the same hazards tended to become recurrent in different scenarios. Thus, for the guidance purposes of the study, the limitation to 4 scenarios was deemed perfectly acceptable. However a systematic safety assessment should better cover also the remaining scenarios and possibly other scenarios not identified at the beginning of the study, to assure that all relevant hazards are identified.

5.3 Classification of hazards by severity

At this stage the workshop participants were confronted with the full list of hazards identified, to classify each of them in terms of severity.

In principle the criteria adopted for the identification of severity was the *ESARR 4 Severity Classification Scheme [Ref: EUROCONTROL SAM FHA Guidance Material: FHA Chap 3 Guidance Material D (Severity Classification Scheme)]*. The scheme is based on a classification in 5 different levels of severity:

1. Accident

2. Serious incidents

3. Major incidents

4. Significant incidents

5. No immediate effect on safety

After a first attempt to directly use the classification scheme and to consider the full range of safety indicators included in it, it was deemed necessary to adopt a simpler classification scheme, distinguishing hazards between *high severity* and *low severity*. Workshop attendees were simply asked to assess the severity of hazards, considering both the perceived severity of consequences and the need for a mitigation mean. High severity hazards were the ones with higher priority for the following discussion about mitigation means (see section 4.5), while low severity hazards were the ones with less priority.

The ranking of severity in 5 different levels was not deemed practical due to the following reasons:

- The limited time available for an analytical use of the severity classification scheme.

- The difficulty of operational experts to classify hazards, taking into account the possible final consequence (accident, serious accident, serious incident, minor incident, significant incident, no immediate effect on safety) without considering the combination with other environmental conditions, which could not be reasonably encompassed in the framework of the present study.

- The difficulty of operational experts to carefully estimating the hazards related to failures of a system they are not used to work with (as explained above, most of the ATCOs switch off the existing STCA, due to its limitations).

However, to ensure consistency with ESARR 4 classification scheme it was then decided to convert all *high severity* hazards as *Severity 3* and all *low severity* hazards as *Severity 4*.

The practical solution identified resulted successful for the purposes of the workshop, as it helped the participants in distinguishing severe hazards from less urgent ones and in prioritizing the following stage of the FHA (identification of mitigation means). Nevertheless a more accurate classification and further time devoted in future to the assessment of severity is deemed beneficial to produce a complete safety case, according to ESARR 4 requirements.

5.4 Identification of mitigation means

The fourth phase was aimed at identifying mitigation means, in term of technical, procedural or training solutions for the specific hazard.

Also in this case a brainstorming approach was adopted. However all participants discussed together in a plenary session, to make sure that sufficient consensus was reached on each solution. The facilitator and the secretary ensured that all the proposed mitigation means were written in a table and shown to all participants through a projector.

As anticipated before not all the hazards were covered and priority was given to hazards classified as *Severity 3*. Furthermore the analysis did not include an estimation of the frequency of hazards and did not aim at identifying specific safety objectives, as in a typical FHA. Thus the priority criterion adopted was only motivated by practical reasons and did not base on a rigorous and systematic assessment of risks.

5.5 Consolidation

The final session was restricted to the facilitator and to the secretary to consolidate the achieved results and ensure that all the hazards and mitigation means were formulated in sufficiently clear and consistent form.

The following results were achieved at the end of the workshop.

- Consideration of scenarios: 4 Out 7 scenarios were analyzed in order to identify hazards
- Hazard identification: 27 hazards identified. 16 Were labelled as “Safety not Enhanced” and 11 as “Negative effect on Safety”
- Classification of severity: 13 out of 27 hazards were classified as *Severity 3*. 14 Out of 27 were classified as *Severity 4*.
- Mitigation means: a set of mitigation means was identified for 16 out of 27 hazards. All *Severity 3* hazards except for one were covered. While specific solutions were identified only for 4 out of the 14 *Severity 4* hazards.

6. DOCUMENTATION OF FHA RESULTS

The FHA results achieved until present have been recorded in an adapted tabular format, compliant with the SAM Methodology *[Ref: Eurocontrol SAM FHA Guidance Material: FHA Chap 3 Guidance Material H (Results Records)]*. The tables presented hereafter provide a documentation of the hazards assessment, including the following items:

Hazard Identifier: Unique hazard identifier (ex: H-OS1-5)

Reference takes the form of H-[Operational Scenario]-[#],

Where :

- H = Hazard;
- [OS #] is a designator signifying a specific scenario in the context of which the hazard was identified;
- [#] is a unique integer assigned to each hazard.

Operational Scenario: name of the analysed operational scenario.

Hazard Title: for each scenario, a synthetic title of the hazard identified.

Hazard Description: for each scenario, a short description of the hazard identified.

Effect of the hazard on operations: description of hazard effects on operations (ATCO, Flight crew, service provision, etc) including the effect on aircraft operations.

Severity Class: the severity of the effects of each hazard, as perceived by the operational experts.

It is to be noted that the following tables do not include a consideration of the environmental conditions which can contribute to the development of each hazard, due the limited time available during the workshop.

As anticipated before, the tables were also divided in 2 main groups, identifying 2 different categories of hazards, in compliance with the EUROCONTROL Safety Assurance Guidance Material for STCA *[Outline Safety Case for Short Term Conflict Alert System]* :

- **Safety Not Enhanced**
  (STCA is potentially providing less than the expected safety benefit)
- **Negative Effect on Safety**
  (STCA is potentially having a negative impact on safety).

STCA FHA – SAFETY NOT ENHANCED

Hazard Ref:	Hazard Title	Hazard Description	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation Means
OS 1 – Flight in Formation/Trail					
H-[OS 1]-1	Partial Transponder failure (lost mode A)	Partial transponder failure (lost mode A) potentially leading to missed genuine alerts, when in conflict with no mode C and unassumed tracks	ATM safety not enhanced by STCA The Controller may become aware too late of a potential conflict to resolve it before a collision scenario develops. There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedure for "manual correlation" to allow the track to be assumed again and STCA being fully active for the track (note that manual correlation is already normal ATCO practice at Semmerzake ATCC)
H-[OS 1]-2	Duplicate Mode A	Duplicate Mode A (due to wrong Mode A assignment by ATCO or to wrong input by pilot), leading to incorrect split track detection, with potential suppression of desirable alerts.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	- Implementation of a logic to check for termination of split track condition on each STCA cycle (proposed solution: indicate in the track format whether the track was updated by a plot or using the predicted position. The STCA alert will be suppressed when a track is not updated using the predicted position). -Use of a duplicate Mode A alert advising the controller when 2 tracks have the same mode A and allowing her/him to assess the situation (note that this feature is already present in the existing system).
H-[OS 1]-3	Lost Wingman	Lost Wingman after loss of visual contact (e.g. due to bad weather conditions) such that the wingman is no longer detected as part of a formation, potentially leading to un-alerted conflict with other un-assumed aircraft.	ATM safety not enhanced by STCA The Controller may become aware too late of a potential conflict to resolve it before a collision scenario develops. There may be a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedure for manually splitting the formation: the formation is split using a 20° angle difference between the elements. All aircraft are instructed to squawk according the manually split flight plan. Then a/c are automatically correlated.

Hazard Ref:	Hazard Title	Hazard Description	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation Means
H-[OS 1]-4	Incorrect military formation detection	Two aircraft falsely detected as a military formation due to similar characteristics such that a genuine conflict is potentially suppressed (e.g. a/c with a difference in flight level more than 1500 feet, with a very similar heading, speed and lateral position)	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
H-[OS 1]-5	Incorrect spilt track detection	Two aircraft falsely detected as a split track due to track creation in proximity (less than 2NM) to an existing system track and either same Mode A or without Mode A, resulting in a genuine conflict being suppressed.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	STCA logic optimization through better tuning of split track detection logic (weighting process of parameters), based on further analysis of traffic samples.
H-[OS 1]-6	Formation split up undetected	Failure to detect when aircraft have left formation, as separation does not exceed the predefined threshold (e.g. 5 NM) resulting in a genuine conflict being suppressed	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Improvement of military formation logic to detect a split of formation, by including a "non-formation" test (the tests checks that aircraft are laterally separated).
OS 2 – Area to Airway					
H-[OS 2]-7	Controller not aware of different parameter sets	Controller mistrust for STCA, due to lack of awareness of the different STCA performances, associated to different parameter sets	ATM safety not enhanced by STCA The Controller may not feel confident when operating at sector capacity thereby increasing risk of contributing to a loss of separation incident.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Specific parts of basic training for controllers to explain the different behaviours of STCA associated to different parameter sets
H-[OS 2]-8 [OS 3] [OS 4]	No or late alert of a level bust with BFL input (1)	Conflict after level bust not alerted or alerted too late, due to alert suppression, after BFL input by ATCO.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Automatic vertical buffer parameter for BFL (e.g. a vertical buffer of 1000ft, will imply that STCA suppression for upper BFL at FL230 is terminated at FL220)

Hazard Ref:	Hazard Title	Hazard Description	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation Means
H-[OS 2]-9	No or late alert of a level bust with CFL input	Conflict after level bust not alerted or alerted too late, due to alert suppression, after CFL input by ATCO.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	New STCA logic to detect when 2 aircraft are heading towards the same flight level and bypass conflict count
H-[OS 2]-10	Wrong BFL/CFL input by controller	Wrong BFL (or CFL) input by ATCO, such that the suppression of STCA persist also after the upper or lower level of a cleared block (or the cleared level) have been passed by the a/c, leading to very short or no warning time	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
OS 3 – Area to Area					
H-[OS 3]-11	No or very short alert of a level bust between two areas	Conflict after level bust not alerted or alerted too late, due to alert suppression after BFL input by ATCO, when the a/c is passing trough the vertical buffer zone between two areas booked one above the other.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	New logic based on passing BFL (and CFL) to STCA, so that the information can be used in the STCA vertical prediction, allowing detection of relevant conflict (e.g. 2 a/c cleared to the same level).
H-[OS 3]-12	No or very short alert of a level bust due to wrong BFL input	Conflict after level bust not alerted or alerted too late, due to wrong BFL input by ATCO, such that there is no or negative buffer zone between two areas booked one above the other and all alerts are suppressed.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Automatic vertical buffer parameter for BFL in order to terminate STCA suppression before the upper or lower BFL is reached (e.g. a vertical buffer of 1000ft, will imply that STCA suppression for upper BFL at FL230 is terminated at FL220).

Hazard Ref:	Hazard Title	Hazard Description	Hazard Effect on ATM	Severity & Exposure Time (Ref SAM Severity Classification Scheme)	Mitigation Means
H-[OS 3]-13	A/c falsely detected as low level VFR	During aerobatics with vertical manoeuvres, wingmen with very little lateral speed potentially detected by mistake as low level VFR, leading to genuine conflicts being suppressed.	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	Procedure for manually split the formation and assigning a discrete SSR code to the wingman (an SSR code which is not a candidate low VFR flight)
OS 4 – STCA inside an Area					
H-[OS 4]-14	Incorrect SSR code list input	Input of an incorrect SSR code list for an aerobatic area, leading to suppression of wanted alerts	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Independent automatic check of the SSR code list which has been loaded
H-[OS 4]-15	Incorrect input of an STCA area	Input (by supervisor?) of an Incorrect STCA area, leading to suppression of wanted alerts	ATM safety not enhanced by STCA The Controller may not become aware of some potential future conflicts or may become aware of them too late, leading to a proportionate increase in the number of conflicts recovered by the pilot or providence to non STCA levels	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Independent check of the STCA areas which have been loaded
H-[OS 4]-16	Controller not aware of STCA suppressed for specific aircraft	Mistrust for STCA, due to controller not aware that STCA is suppressed for two aircraft undergoing exercises	ATM safety not enhanced by STCA The Controller may not feel confident when operating at sector capacity thereby increasing risk of contributing to a loss of separation incident.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	Indication in the track symbol that STCA has been suppressed for the specific track (e.g. different shape of the label)

STCA FHA – NEGATIVE EFFECTS ON SAFETY

Hazard Ref:	**Hazard Title**	**Hazard Description**	**Hazard Effect on ATM**	**Severity & Exposure Time (Ref SAM Severity Classification Scheme)**	**Mitigation Means**
OS 1 – Flight in Formation/Trail					
H-[OS 1]-17	Total Transponder failure (lost mode C and mode A)	Transponder failure (lost mode C and mode A) potentially leading to: - missed genuine alerts, when in conflict with no mode C and unassumed a/c - nuisance alerts when in conflict with Mode C equipped and correlated a/c, due to lack of vertical prediction testing	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	- Procedure for "manual correlation" to allow the track to be assumed again and STCA being fully active for the track (note that manual correlation is already normal ATCO practice at Semmerzake ATCC) - Display the primary track as a type of "emergency track" on all CWPs.
H-[OS 1]-18	Partial Transponder failure (lost mode C)	Partial transponder loss (lost mode C) potentially leading to: - missed or late alerts (when in conflict with assumed mode C tracks), due inappropriate parameters applied - nuisance alerts when (when in conflict with assumed mode C tracks), due to lack of vertical prediction testing by STCA - missed alert (when in conflict with unassumed or no mode C tracks)	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 3 Resolution and/or recovery functions partially impaired. Possible significant increase in workload or stress, particularly at peak traffic times.	- Display the primary track as a type of "emergency track" on all CWPs.
H-[OS 1]-19	Split track	Split track due to incorrect plot to track association (one or more plots not associated with an existing system track) leading to false alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*

Hazard Ref:	**Hazard Title**	**Hazard Description**	**Hazard Effect on ATM**	**Severity & Exposure Time (Ref SAM Severity Classification Scheme)**	**Mitigation Means**
H-[OS 1]-20	Un-wanted alerts between in-trail flights	In trail flights not detected by formation flight suppression logic leading to nuisance alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
OS 2 – Area to Airway					
H-[OS 2]-21	Erased BFL on handover	Erased BFL after handover leading to nuisance alerts (next controller is forced to reassign the BFL)	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
H-[OS 2]-22	Wrong BFL/CFL input by controller	Wrong BFL (or CFL) input by ATCO, such that STCA is not suppressed when the a/c is still inside a cleared block (or above/below a cleared level), leading to nuisance alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
OS 3 – Area to Area					
H-[OS 3]-23	Unexpected wider parameters inside a booked area	Unexpected wider parameters inside a booked working area due to misunderstanding with AMP (Airspace Management Program), leading to an increased number of nuisance alerts (e.g. big working area split in two smaller areas with buffers, ATCO not aware of it)	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
OS 4 – STCA inside an Area					

Hazard Ref:	**Hazard Title**	**Hazard Description**	**Hazard Effect on ATM**	**Severity & Exposure Time (Ref SAM Severity Classification Scheme)**	**Mitigation Means**
H-[OS 4]-24	Garbled Mode A code	Mode A code garble such that a track planned to be part of a training SSR code list, will not be detected by STCA as part of that list, potentially leading to nuisance alerts.	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
H-[OS 4]-25	Wrong SSR code assignment	Wrong SSR code assigned by ATCO such that a training aircraft is labelled as a non training aircraft, potentially leading nuisance alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
H-[OS 4]-26	Wrong SSR code request	Wrong SSR code requested by pilot such that a training aircraft is labelled as a non training aircraft, potentially leading nuisance alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*
H-[OS 4]-27	Wrong SSR code input	Wrong SSR code input into transponder by pilot, such that a training aircraft is labelled as a non training aircraft, potentially leading nuisance alerts	Negative effects on ATM Safety. The Controller's workload increased through assessing Alerts for validity. This may distract the Controller to the point that there may be a proportionate increase in the number of conflicts to *higher* than non STCA levels.	Severity 4 Resolution and/or recovery functions slightly impaired. Possible slight increase in workload or stress, particularly at peak traffic times.	*Mitigation not identified*

7. CONCLUSIONS

The adopted approach yielded a successful result, considering both the large number of hazards, the mitigation means identified and the high quality of contribution offered by attendees with a wide variety of backgrounds.

The performed FHA had precise limitations in its scope; i.e. the assessment of the frequency of hazards was not performed and specific safety objectives were not identified. However the STCA managers of ATCC Semmerzake had at the same time a concrete opportunity for testing the SAM methodology and a possibility to assess the safety implications of their STCA, once the proposed solutions for enhancing and optimizing the current system will be implemented.

As a consequence of the work, the mitigation means identified during the FHA workshop have been used as an input to update the recommendations included in the previous report of the same document set (see Appendix D-1: Optimisation of STCA for ATCC Semmerzake). While the hazards identified and the assessment of their severity can be used as first step for ATCC Semmerzake to define specific safety objectives and to produce a safety case according to ESARR 4 requirements.

END OF DOCUMENT