

# EUROCONTROL



**EUROCONTROL Guidance  
Material for Minimum Safe Altitude  
Warning  
Appendix D-2: Functional Hazard  
Assessment of MSAW for  
Skyguide**

|                       |   |                         |
|-----------------------|---|-------------------------|
| <b>Edition Number</b> | : | <b>1.0</b>              |
| <b>Edition Date</b>   | : | <b>19 May 2009</b>      |
| <b>Status</b>         | : | <b>Released Issue</b>   |
| <b>Intended for</b>   | : | <b>CND Stakeholders</b> |



## DOCUMENT CHARACTERISTICS

| TITLE   |                        |               |
|---|------------------------|---------------|
| <b>EUROCONTROL Guidance Material for Minimum Safe Altitude Warning<br/>Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide</b>  |                        |               |
| <b>Document Identifier</b>  | <b>Edition Number:</b> | 1.0           |
| EUROCONTROL-GUID-127  | <b>Edition Date:</b>   | 19 May 2009   |
| Abstract  |                        |               |
| <p>This document describes a Functional Hazard Assessment made to identify possible hazards associated to the introduction a new improved MSAW system in Skyguide, as proposed in the companion case study document "Appendix D-1 : Enhancement of MSAW for Skyguide". Such a study has investigated the feasibility of extending the implementation of MSAW beyond its current boundaries and the effectiveness of using of digital terrain data. The potential hazards identified in the present study, however, pertain to the Skyguide MSAW system as a whole and are not exclusively covering the safety implications of the two proposed innovations.</p> |                        |               |
| Keywords  |                        |               |
| Safety Nets<br>MSAW<br>DTED<br>AMP  |                        |               |
| <b>Contact Person(s)</b>  | <b>Tel</b>             | <b>Unit</b>   |
| Ben Bakker  | +32 2 72 91346         | CND/COE/AT/AO |

| STATUS, AUDIENCE AND ACCESSIBILITY |                                     |   |                                     |                                |                                     |
|------------------------------------|-------------------------------------|---|-------------------------------------|--------------------------------|-------------------------------------|
| Status                             |                                     | Intended for  |                                     | Accessible via                 |                                     |
| Working Draft                      | <input type="checkbox"/>            | General Public  | <input type="checkbox"/>            | Intranet                       | <input type="checkbox"/>            |
| Draft                              | <input type="checkbox"/>            | CND Stakeholders  | <input checked="" type="checkbox"/> | Extranet                       | <input type="checkbox"/>            |
| Proposed Issue                     | <input type="checkbox"/>            | Restricted Audience   | <input type="checkbox"/>            | Internet (www.eurocontrol.int) | <input checked="" type="checkbox"/> |
| Released Issue                     | <input checked="" type="checkbox"/> | <i>Printed &amp; electronic copies of the document can be obtained from ALDA (see page iii)</i> |                                     |                                |                                     |




| ELECTRONIC SOURCE |                          |         |
|-------------------|--------------------------|---------|
| <b>Path:</b>      | \\HHBRUNA02\bakkerb\$\QC |         |
| Host System       | Software                 | Size    |
| Windows_NT        | Microsoft Word 10.0      | 1013 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](mailto: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                       | <br>Ben Bakker       | 19-5-2009 |
| Head of ATC Operations and Systems Unit | <br>Martin Griffin | 19-5-2009 |
| Deputy Director Network Development     | <br>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            | 19-5-2009    | First released issue | All            |
|                |              |                      |                |
|                |              |                      |                |
|                |              |                      |                |
|                |              |                      |                |

# CONTENTS

|   |            |
|---|------------|
| <b>DOCUMENT CHARACTERISTICS.....</b>                    | <b>ii</b>  |
| <b>DOCUMENT APPROVAL.....</b>                           | <b>iii</b> |
| <b>DOCUMENT CHANGE RECORD.....</b>                      | <b>iv</b>  |
| <b>FOREWORD.....</b>                                    | <b>1</b>   |
| <b>1. INTRODUCTION.....</b>                             | <b>3</b>   |
| 1.1 Overview of the Study.....                          | 3          |
| 1.2 Report Structure.....                               | 3          |
| <b>2. THE MSAW UNDER ASSESSMENT.....</b>                | <b>4</b>   |
| 2.1 Current MSAW Characteristics and Limitations.....   | 4          |
| 2.1.1 MSAW Polygons.....                                | 4          |
| 2.1.2 Track Eligibility and Inhibition.....             | 5          |
| 2.1.3 Human-Machine Interface.....                      | 6          |
| 2.1.4 MSAW Performance.....                             | 6          |
| 2.2 Summary of Recommendations from the Case Study..... | 7          |
| 2.3 Assumptions on the new MSAW to be assessed.....     | 7          |
| <b>3. FHA SCOPE AND METHOD.....</b>                     | <b>9</b>   |
| 3.1 Objectives of the Assessment.....                   | 9          |
| 3.2 Hazard Elicitation Method.....                      | 10         |
| 3.2.1 Keywords guided functional analysis.....          | 11         |
| 3.2.2 Scenario based operational analysis.....          | 12         |
| <b>4. ORGANISATION OF THE WORKSHOP.....</b>             | <b>15</b>  |
| 4.1 Introduction and description of the system.....     | 16         |
| 4.2 Identification of hazards.....                      | 16         |
| 4.3 Classification of hazards by severity.....          | 17         |
| 4.4 Identification of mitigation means.....             | 18         |
| 4.5 Consolidation.....                                  | 18         |
| <b>5. DOCUMENTATION OF FHA RESULTS.....</b>             | <b>19</b>  |
| 5.1 FHA Tabular Format.....                             | 19         |

|           |   |           |
|-----------|---|-----------|
| 5.2       | Category of Hazards Identified .....  | 19        |
| <b>6.</b> | <b>CONCLUSIONS.....</b>   | <b>32</b> |
| 6.1       | Input for an MSAW Safety Case .....   | 32        |
| 6.2       | Safety Feedback to MSAW Enhancement Recommendations .....                       | 32        |
| 6.2.1     | Undesired Side Effects of the Addressing Mechanism .....                        | 33        |
| 6.2.2     | Combination of MSAW alerts with other alerts.....                               | 33        |
| 6.2.3     | Terrain collision geometries potentially challenging the DTED performance ..... | 34        |

## FOREWORD

Skyguide's MSAW system was installed in 1999. It is currently applied in the vicinity of Geneva and Zurich airports. Despite having some technical limitations, the system is in daily operational use and it is known that controllers trust it.

In the first half of 2008, Skyguide and EUROCONTROL, supported by QinetiQ and Deep Blue, collaborated to study possible enhancements of the MSAW function.

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

- Appendix D-1: Enhancement of MSAW for Skyguide
- Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide [This Document]

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

Note however that specific solutions identified in the document should not be adopted without performing similar analysis to determine their applicability in the target environment.





## **1. INTRODUCTION**

### **1.1 Overview of the Study**

The present Functional Hazard Assessment (FHA) complements the Skyguide MSAW case study included in the companion guidance document named: “Appendix D-1: Enhancement of MSAW for Skyguide”.

Skyguide’s MSAW system was installed in 1999 and it is currently applied in the vicinity of Geneva and Zurich airports. It is in daily operational use and it is known that controllers trust it. Still, the system has some shortcomings which are addressed in the case study document.

While the case study focuses on the possible solutions to enhance the current MSAW installation and to extend its geographical coverage, this report identifies the potential risks for safety associated to the implementation and operational use of MSAW in the ATM system. It is intended as an example for ANSPs which are currently planning to design and implement a new MSAW, in compliance with the ECIP Objective ATC02.6.

As for all the new systems being introduced, the FHA is essential part of the overall Safety Case that ANSPs are required to set up and maintain according to ESARR 4 requirements. Guidance on how to perform a safety case can be found in the document “EUROCONTROL Guidance Material for MSAW – Appendix B: Safety Assurance”.

### **1.2 Report Structure**

Chapter 2 describes the key element of the MSAW system which is assessed in the following part of the report. The description includes both the new MSAW features proposed in the case study and the current MSAW characteristics that will be retained in the new system.

The scope and method adopted for the FHA and the organization of the FHA workshop are described respectively in Chapter 3 and 4.

Finally chapter 5 presents a record of the results achieved with the MSAW FHA workshop made at Geneva ACC.

Conclusions and recommendation are drawn in chapter 6.

## **2. THE MSAW UNDER ASSESSMENT**

### **2.1 Current MSAW Characteristics and Limitations**

This section summarizes the characteristics of the current Skyguide MSAW, before passing to the description of the enhanced system proposed in the MSAW case study and analyzed through FHA in the present report.

Although the FHA is focused on the proposed future MSAW, a basic knowledge of the current system is essential background information to understand the hazards hereafter identified.

The readers who have already a good understanding of the companion document “Appendix D-1: Enhancement of MSAW for Skyguide” are suggested to skip to section 2.3.

#### **2.1.1 MSAW Polygons**

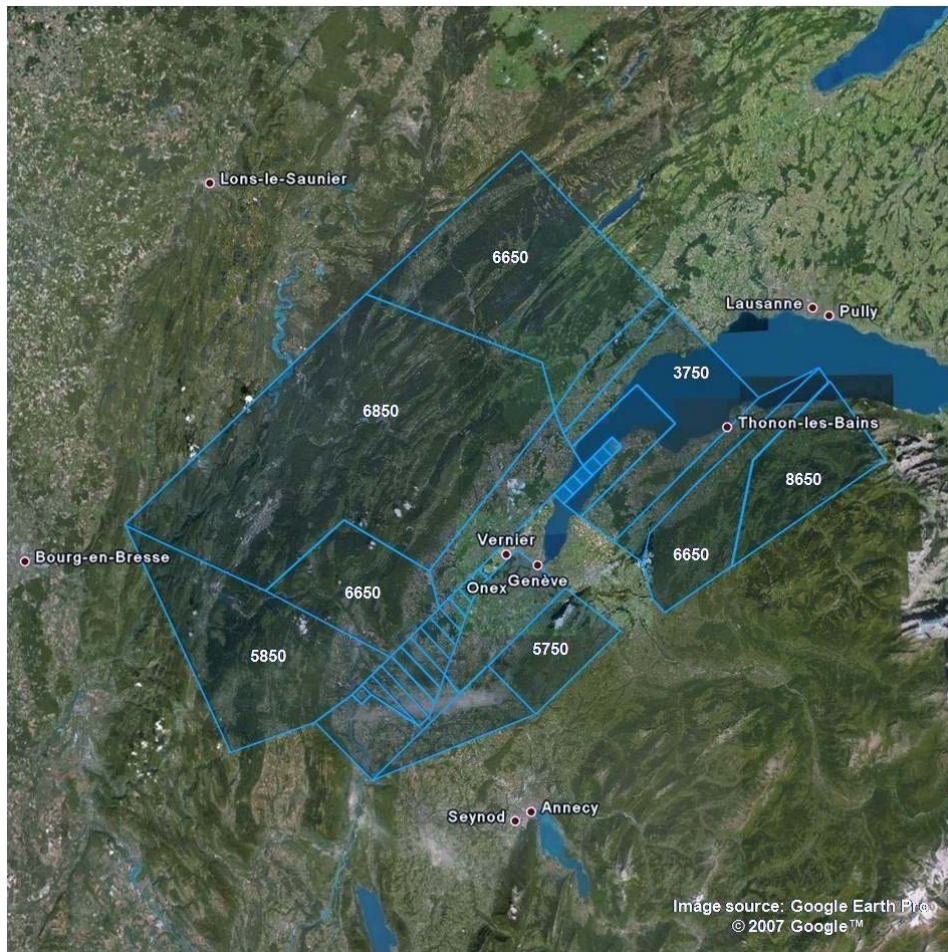
As described in the case study document, Skyguide’s current MSAW system works on the basis of detecting aircraft tracks that penetrate predefined volumes of airspace. These MSAW volumes have been carefully defined off-line by Skyguide engineers with the assistance of experienced controllers.

The MSAW volumes for Geneva are shown in Figure 2-1. They extend to a maximum of 30 NM from the airport. Each MSAW volume is defined as a polygon with a fixed ceiling height. The majority of the coverage is based on pre-defined Minimum Vectoring Altitudes (MVAs) with each MSAW polygon ceiling set 350ft below the respective MVA.

In addition, Skyguide employ the MSAW function for Approach Path Monitoring (APM). This has been achieved by defining numerous small MSAW polygons along the line of the runway final approach paths (GVA RWY 23 and 05). When viewed in 3D, these small polygons appear like a staircase.

A hole in the MSAW polygon coverage is present close to Geneva. This gap in the polygons is designed to prevent nuisance alerts for VFR aircraft on arrival to or departure from Annemasse airport.

No prediction is applied in the MSAW system. If an eligible aircraft penetrates one of the defined MSAW volumes then an alert is generated which may then be displayed to the controller, depending on whether the controller has already manually inhibited the track from MSAW alerting.



**Figure 2-1: The current MSAW coverage in the Geneva area**

### 2.1.2 Track Eligibility and Inhibition

An aircraft is eligible for MSAW processing if it is correlated with a flight plan, and its SSR code is not on a pre-defined VFR or Military (MIL) code list. On the face of it, this scheme should work well. However, there is sometimes a mismatch between the flight rules for an aircraft and the allocated SSR code. For example, a flight may be allocated an SSR code which indicates IFR, yet the flight takes off VFR joining IFR later. In other cases a flight may be squawking an SSR code indicating IFR but may then for some reason make a VFR approach, and as a consequence proceed intentionally below the MVA into an MSAW polygon.

The controller has the facility to inhibit MSAW for selected tracks. This is usually done for visual approaches and VFR traffic squawking an IFR SSR code (joining flights). The controller knows these flights will remain close to the terrain to have visual references, and therefore an MSAW alert would just be a distraction.

### 2.1.3 Human-Machine Interface

The MSAW provides both a visual and an audible alert. The visual part consists in the concerned label track becoming red. The audible part consists in a recorded voice saying: “altitude...altitude”.

As anticipated, controllers have the possibility to inhibit MSAW for a specific track in two different ways: a) before an alert is activated, by selecting the option “Disregard”; b) after an alert is activated, by selecting the option “Acknowledge”.

The screenshots below (Figure 2-2) show how the concerned track is displayed on the CWP in the different conditions.

In the upper sequence of three pictures the MSAW alert has not been triggered yet and we see what happens when the controller decides to inhibit the MSAW alerting (MSAW deactivated) and then to reactivate it (MSAW reactivated). On the other hand, in the two lower pictures we see what happens when an MSAW alert is triggered by the system (MSAW alert unacknowledged) and subsequently acknowledged by the controller (MSAW alert acknowledged).



Figure 2-2: Deactivation, reactivation and acknowledgment of MSAW

### 2.1.4 MSAW Performance

The current MSAW system generates around 15 alerts per day on average. Normally, however, not all of these alerts are displayed at the CWP, since the controller has the facility to disable MSAW for specific tracks, and also to acknowledge an alert that is in progress.

Whether these alerts could be defined as a nuisance or not is debatable, since the controllers appear to have learnt to expect a small number of unnecessary alerts which they can easily suppress.

Most essentially, verbal comments from controllers indicate that they trust the current MSAW system.

Nevertheless, as with all safety nets, there is an unavoidable risk that an increased number of unnecessary alerts could lead to controllers becoming desensitized to alerts, and hence not paying due attention to genuine alerts when they occur. This is why a considerable part of the Case Study has been devoted to measure the number of MSAW alerts, as well as to consider their nature.

## 2.2 Summary of Recommendations from the Case Study

The Case Study aimed at finding answers to the following key questions:

- Scalability: what needs to change in the existing MSAW implementation to extend its geographical coverage to the whole Skyguide area of interest?
- Volumes (hand designed polygons) versus Digital Terrain Elevation Database (DTED): what is the best option for Skyguide?
- Detection versus prediction: what is the best option for Skyguide?
- Operational Philosophy: are the current key choices with respect to track eligibility sustainable?

In essence the study has concluded that extending the Skyguide MSAW coverage is feasible using either the MSAW Polygons or the DTED. A comparative analysis of the alerting performance, however, has shown that **MSAW system is likely to perform much more satisfactorily with the use of DTED data and prediction.**

Furthermore the alert rate statistics for the various types of flight (correlated/uncorrelated; IFR/VFR/MIL) has shown that the current Skyguide philosophy of **subjecting only correlated IFR flights to MSAW succeeds in maintaining a relatively low alert rate.**

## 2.3 Assumptions on the new MSAW to be assessed

At the time this report is being written, a final decision on the new MSAW design has still to be taken by Skyguide. Performing an FHA, however, requires making some precise assumptions on how the system under assessment is expected to function. The assumptions help both technical and operational experts in anticipating possible malfunctions and errors whose effects should be carefully analyzed and considered for mitigation.

The following characteristics have been defined for the new MSAW to be assessed.

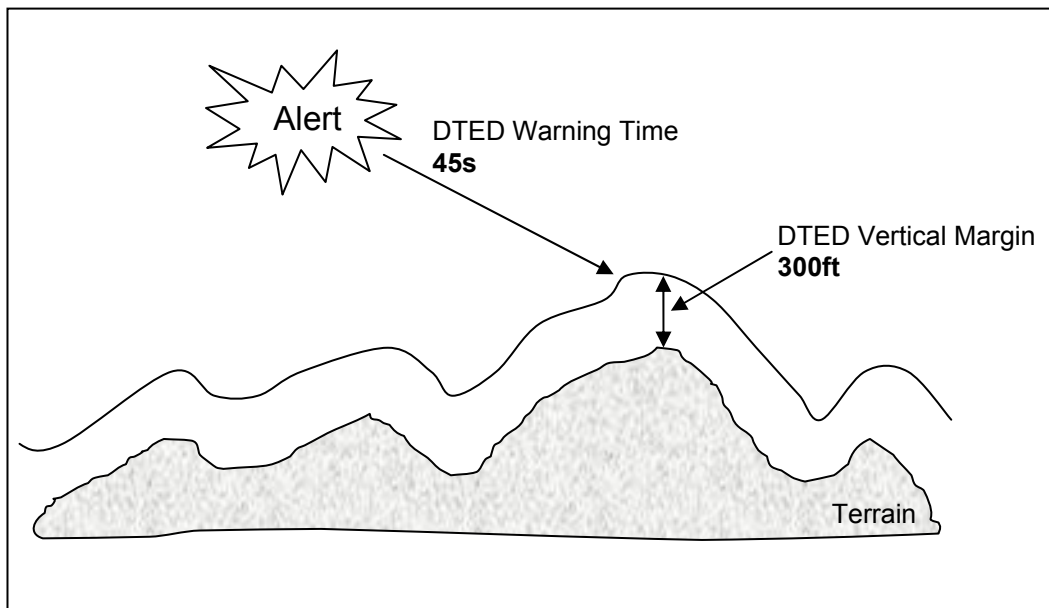
The MSAW processing will be entirely based on a DTED (see Figure 2-3). Essential parameters will be:

- Vertical Margin: **300ft**
- DTED Warning Time: **45s**

The MSAW alerts will be addressed only to the CWP of the ATCO who has assumed the track which is triggering the alert.

As for the current MSAW, **only the IFR correlated track will be processed.**

The **essential elements of the current HMI will be retained**, including the possibility for controllers to disable MSAW for a specific track -either before or after an alert is triggered- and to re-enable it after it as been acknowledged/ deactivated.



**Figure 2-3: A representation of the assumed DTED based MSAW**

### 3. FHA SCOPE AND METHOD

#### 3.1 Objectives of the Assessment

In the context of this study the FHA aims at identifying the potential hazards associated to the introduction of the enhanced MSAW (E-MSAW) in the Skyguide ATM system.

More specifically the study addresses 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 MSAW.
- The **hazards** potentially determining a **negative effect on safety** as opposed to the operational condition without MSAW.
- 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 FHA workshop to the issues listed above. The definition of safety objectives, as a typical FHA should normally encompass, is not included.

It is also worth nothing that although the study considers with special interest the new features proposed in the MSAW case study, such as the alerting behaviour based on DTED, the system under assessment is the whole MSAW, including the new features.

In practical terms, the FHA is performed considering all the hazards from scratch, as if no implemented MSAW were actually available. Two main reasons justify this methodological choice:

- The current MSAW system was implemented in 1999 and there is no previous FHA specifically available for MSAW.
- An assessment considering the whole MSAW system - and not only the proposed innovative features - can be better used as reference

material for other ANSPs which are currently planning to implement a new MSAW system with similar characteristics<sup>1</sup>.

Based on these considerations, the hazards hereafter identified pertain to both the future enhanced MSAW characteristics and the characteristics of the current system that will be retained in the enhanced system.

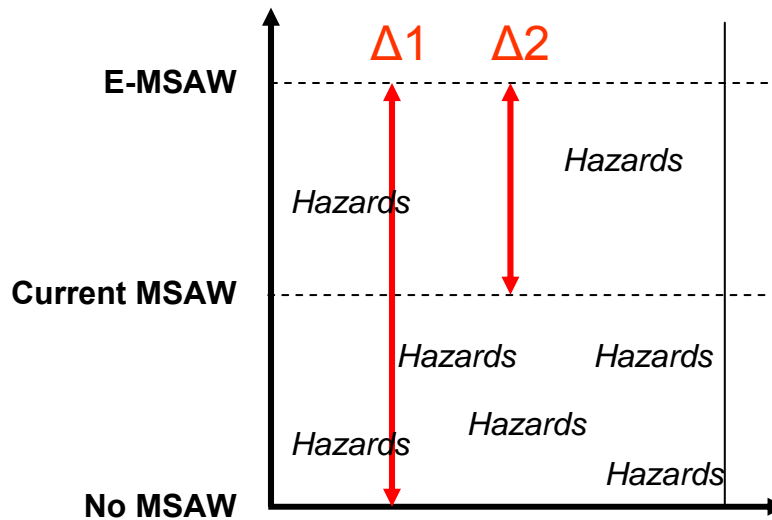


Figure 3-1: A representation of the difference between  $\Delta 1$  and  $\Delta 2$  hazards

The Figure 3-1 shows how the majority of hazards is associated to the delta between the *No MSAW* and the *E-MSAW* condition ( $\Delta 1$ ). On the other hand, a subset of hazards pertains only to the delta between the *Current MSAW* and the *E-MSAW* condition ( $\Delta 2$ ). For the sake of clarity these former hazards will be marked with a  $\Delta 2$  in the final hazard documentation reported in chapter 5.

### 3.2 Hazard Elicitation Method

A hazard is a potentially unsafe condition resulting from failures, malfunctions, external events, errors or a combination thereof that may contribute to cause an incident or accident. In order to identify hazards, the present study adopts in a slightly simplified manner the methods and techniques proposed by the EUROCONTROL Safety Assessment Methodology (SAM). As suggested in the SAM guidance material, the identification of hazards requires a combination of at least two complementary approaches.

- A functional approach: consider the various way in which each individual function of the system under analysis can fail

<sup>1</sup> Note that although the study identifies all hazards from scratch, assuming the introduction of a completely new MSAW system, the FHA can of course benefit of the significant experience made until present by the Skyguide operational and technical personnel.



- **A brainstorming approach:** organize brainstorming session to look for “functionally unimaginable” hazards by assessing normal, abnormal and particular combination of unrelated event scenarios.

Both the approaches have been followed in a one day and half FHA workshop organized at Skyguide Geneva ACC in July 2008 (see further details in the following chapter 4). Two different techniques, each corresponding to one of the two approaches, were actually adopted to support the workshop attendees in the identification of hazards. These techniques are briefly described in the following subsections.

### 3.2.1 Keywords guided functional analysis

This technique consists in analysing the functional components of the system under assessment and in considering the different ways in which they can fail, taking into account both technical failures and human errors. The analysis is supported by a checklist of ‘prompts’ or keywords’ suggesting different failure modes to be considered.

During the workshop at Geneva ACC the attendees were provided with the checklist shown in Table 3-1. It is an adaptation of the checklist illustrated in the SAM Methodology guidance material [Ref: Eurocontrol SAM FHA Guidance Material: FHA Chap 3 Guidance Material B1 (Identification of Failure Modes, External Events and Hazards)].

The upper part of the checklist suggests the two main drivers for a hazard to happen: ATM equipment components on the left side and human operators on the right side. As most of the hazards are typically identified at the boundary of the system under assessment, also some of the components/roles that receive or provide input to the MSAW and that are considered to influence its functioning are mentioned (e.g. the transponder and the CWP HMI on the left side and the controller or the pilot on the right side).

The lower part of the checklist suggests different failure modes of the components/roles indicated above. In analogy with the upper part, technical failure modes are listed on the left side and human error modes are listed on the right side.

It is worth specifying that the checklist should not be used in a rigid way. It can be either used in a systematic manner by considering all possible failure modes or as simple additional support when the team of evaluators is at risk of getting stuck in the analysis. The list of items is of course not exhaustive and should be adapted or integrated to better fit with the specific objectives of the assessment. On the other hand, the list should not constrain the analysis in case some of the components and failure modes do not apply to the specific system under assessment

Finally, not mentioned in the checklist, FHA facilitators should be also encouraged to think about *external events* (e.g. severe weather phenomena) which can contribute to a failure condition or hazard.

| ATM EQUIPMENT COMPONENT   | OPERATOR  |
|---|---|
| <p><b>MSAW</b></p> <p>Other components or functions related to the MSAW (e.g. Transponder, CWP HMI, QNH, etc).</p>  | <p><b>Controller</b></p> <p><b>Pilot</b></p> <p>Other operators (whose actions affect the MSAW functioning)</p>   |
| <i>POSSIBLE FAILURE MODES</i>   | <i>POSSIBLE ERRORS</i>  |
| <p><b>Total loss</b></p> <p><b>Partial loss</b></p> <p><b>Erroneous updating</b></p> <p><b>Erroneous setting</b></p> <p><b>Error of input/ output:</b></p> <ul style="list-style-type: none"> <li>- missing data (partial loss, total loss)</li> <li>- detected erroneous/corrupted data (not credible error/corruption)</li> <li>- undetected erroneous/corrupted data (credible error/corruption)</li> <li>- out of sequence</li> <li>- out of range</li> </ul> | <p><b>Omitted operation</b></p> <p><b>Delayed operation (too late)</b></p> <p><b>Premature operation (too early)</b></p> <p><b>Inadvertent operation</b></p> <p><b>Modified operation</b></p> <p><b>Violation of operation (Routine or unintentional)</b></p> <p><b>Used beyond intent</b></p> <p><b>Misunderstood</b></p> <p><b>Misheard</b></p> <p><b>Failure to start/stop</b></p> <p><b>Failure to switch</b></p> |

**Table 3-1: The checklist to support the MSAW related hazard identification**

### 3.2.2 Scenario based operational analysis

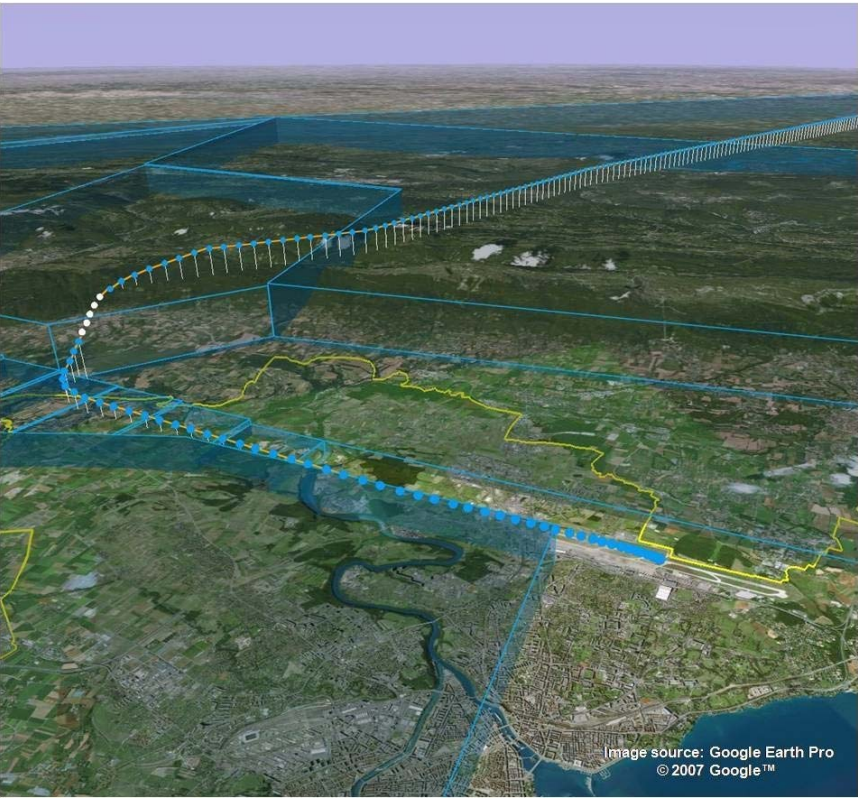
The scenario based analysis consists in encouraging a group of domain experts with different backgrounds –both operational and technical– in brainstorming about possible hazardous situations related to the system under assessment in specific operational scenarios. As matter of fact, the most insidious hazards are not caused by single functional failures which can be more easily mitigated. Rather they are induced by dysfunctional interactions between perfectly working elements of the ATM system, including equipment, procedure and human operators.

In the case of MSAW, for example, the evaluators should reflect on operational situations in which a/c are vectored in proximity of the minimum safe altitude and in which the MSAW can play an important role in mitigating the risks of a possible CFIT. This kind of analysis allows particularly the operational experts to reason in terms of their concrete experiences with situations potentially challenging the MSAW supporting role, rather than in the abstract and logical terms of a functional analysis.

The elements taken into consideration are not only the technical components of the system and their possible failures, but also the other contextual factors affecting the MSAW performance, such as the specific geographical characteristics of the area covered by the MSAW, the aerodromes' position, the airspace configuration, the runway design, the typical traffic flows, the working methods and procedures adopted by the ANSP, etc. The hazards caused by possible critical interactions between these elements, including the MSAW, can only be envisaged if the operational expertise is adequately conveyed into the discussion by means of representation of realistic operational scenarios.

The following Table 3-2 shows an example of a scenario representation used during the FHA Workshop in Geneva ACC. It is a departure from Geneva airport from a specified runway (RWY23) and with a specified SID (DIPIR 4A). It shows an operational circumstance in which ATCOs are typically required to disable the track from the MSAW alerting in case the a/c is an IFR flight in order to inhibit a possible nuisance alert. The picture in the middle shows part of the geography in the Geneva area, the shape of the current MSAW Polygons and the trajectory of an a/c which partially infringing one of them. The textual description highlights the expected behaviour of both the current and future MSAW and shows how the DTED based enhanced MSAW would not have triggered and alert in this case.

During the brainstorming sessions of the FHA workshop the attendants were asked to identify possible hazards which could potentially occur in this scenario, as well as in others. The possibility to focus the attention each time on the representation of a specific situation helped the participants in having a shared representation of the hazards which were discussed, taking into account the combination of more contextual factors and not only the MSAW function in isolation.

| <b>GVA Departure 1</b>               |  |
|--------------------------------------|--|
| <b>Description</b>                   | <b>Traffic departing GVA Airport RWY23 on the SID DIPIR 4A direction north, turn initiated below the minimum SID depicted altitude</b>   |
| <b>Operational implications</b>      | <ul style="list-style-type: none"> <li>▪ Likely to be a distraction for the controller or extra workload if the controller disables the track from MSAW alerting</li> <li>▪ Possible confusion for controller to distinguish between VFR and IFR flights?</li> </ul>   |
| <b>Implications for current MSAW</b> | <ul style="list-style-type: none"> <li>▪ MSAW polygons alerting when infringed (normally 350ft below the MVA)</li> <li>▪ Alerts only generated for aircraft squawking IFR codes</li> <li>▪ VFR/MIL not eligible for alerting</li> <li>▪ ATCO allowed to disable MSAW for individual tracks</li> </ul>  |
| <b>Implications for the E-MSAW</b>   | <div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  <p style="font-size: small; text-align: right;">Image source: Google Earth Pro<br/>© 2007 Google™</p> </div> <div style="flex: 1; padding-left: 10px;"> <p><b>Example</b></p> <ul style="list-style-type: none"> <li>▪ <b>Polygon alert:</b><br/>10:09:04 for a duration of 20 seconds</li> <li>▪ <b>Height of Aircraft:</b><br/><b>6270ft</b> at the time of alert</li> <li>▪ <b>Mode A Code:</b><br/>5775</li> <li>▪ <b>Polygon Identity :</b><br/>MSAWGCR<br/>(height of polygon: 6650ft)</li> <li>▪ <b>4 modelled polygon alerts</b> on 1<sup>st</sup> September 2007</li> </ul> </div> </div> <ul style="list-style-type: none"> <li>▪ <b>No DTED alert</b></li> <li>▪ DTED alerting based on the following parameters                             <ul style="list-style-type: none"> <li>○ <b>Warning Time:</b> 45s</li> <li>○ <b>Vertical Margin 1:</b> 300ft</li> </ul> </li> <li>▪ Alerts only generated for aircraft correlated IFR tracks</li> <li>▪ VFR/MIL not eligible for alerting</li> <li>▪ ATCO allowed to disable MSAW for individual tracks (and to re-enable them afterwards)</li> <li>▪ Inhibition area defined for Geneva</li> </ul> |

**Table 3-2: An example of operational scenario used during the FHA workshop**

#### 4. ORGANISATION OF THE WORKSHOP

The organisation of an FHA workshop always requires the involvement of a team of people with an adequate mix of different backgrounds, in order to facilitate the brainstorming activity through the confrontation of different points of views. These should be covered by representatives of at least three different roles:

- Operational experts
- Technical experts
- Safety analysts.

The workshop organized in Geneva involved a team of 5 people, including 3 participants from Skyguide and 2 from EUROCONTROL:

- An ATM procedures and safety nets expert with long-lasting experience as ATCO (from Skyguide)
- A currently operational, very experienced ATCO (Skyguide)
- A technical expert, with knowledge of the local MSAW system (Skyguide)
- A technical expert, who had conducted for EUROCONTROL the MSAW case study included in Appendix D-1 (from QinetiQ)
- A safety expert with background in human factors, who played the role of workshop facilitator (from Deep Blue).

The program of the Workshop included 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 sub-sections provide a very quick description of the methodological process, as it was specifically deployed during the meeting in

Geneva<sup>2</sup>. The reader who is only interested in the documentation of FHA results should skip to section 5.

#### **4.1 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.

Adequate time was then spent to present the main characteristics of the system under investigation (see chapter 2). Although the people involved in the workshop had all a good knowledge of the related MSAW case study, the basic functioning principles were again presented in detail, to make sure that all participants shared a common view of the proposed E-MSAW.

This phase is essential to make sure that all attendants will be actually in condition to contribute to the hazard identification phase. Furthermore it can easily happen that the system about to be assessed is still under-defined or subject to different interpretations by the stakeholders. Thus, in case some assumptions are still required on the future design choices, it is essential that these assumptions will be made as more explicit as possible to the participants.

#### **4.2 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 checklist to be used as a support for generating ideas (see sec. 3.2.1) and with the structure of a typical table describing an operational scenario (see sec. 3.2.2).

*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)*

---

<sup>2</sup> For further information on how to organize an FHA session see the following reference: *Eurocontrol SAM FHA Guidance Material: FHA Chap 3 Guidance Material B2 ("Functionally Unimaginable" hazards – FHA Session)*.

After a specific scenario was analyzed in sufficient detail, the brainstorming session began, allowing all participants propose ideas about possible hazards. The facilitator had the responsibility to make a unified list of hazards, showing it to all participants through a projector. One of the technical experts played also the role of secretary to help the facilitator in maintaining and consolidating the list of hazards.

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 anyhow note of it for further discussion during the following phases of brainstorming.

### 4.3 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 for at least two reasons:

- The limited time available for a 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.

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.

#### **4.4 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, making 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.

#### **4.5 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 results achieved at the end of the workshop are reported in Chapter 5.



## 5. DOCUMENTATION OF FHA RESULTS

### 5.1 FHA Tabular Format

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 hazard assessment, including the following items:

Hazard Identifier: a unique progressive number

Hazard Title: a title of the hazard identified indicating the main causal factor.

Hazard Description: 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.

Hazards are also grouped in different categories, whose titles are highlighted in the rows in grey.

### 5.2 Category of Hazards Identified

Hazards are grouped in the following categories, according to the kind of alerting performance of MSAW in the specific hazardous situation:

- Loss of function (3)
- Missed alert (13)
- Incomplete alert (2)
- Delayed alert (4)
- Nuisance alert (7)
- Incorrect addressing of alert (3)
- Alert combined with other alerts (5)

In compliance with the EUROCONTROL Safety Assurance Guidance Material for MSAW [*Outline Safety Case for Minimum Safe Altitude Warning*], the FHA tables also distinguish between 2 main groups of hazards:

- **Safety Not Enhanced** (Success Case)
- **Negative Effect on Safety** (Failure Case).

The first group includes the hazards for which it is considered that the MSAW is potentially providing to the ATM system less safety benefit than expected.

The second group includes the hazards for which it is considered that the MSAW is potentially having a negative impact on the safety of the ATM system, with respect to the pre-MSAW condition.

Finally, as explained in 2.3, a “Delta 2” label has been added to each hazard pertaining only to the delta between the *Current MSAW* and the *E-MSAW* condition ( $\Delta 2$ ).

**MSAW FHA – SAFETY NOT ENHANCED**

| Hazard ID:              | Hazard Title   | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means   |
|-------------------------|--|---|---|--|--|
| <b>Loss of function</b> |  |   |   |  |  |
| 1.                      | <b>Total loss</b> of MSAW  | The MSAW does not trigger any alert in case of a/c infringing or about to infringe the vertical margin in all the MSAW coverage area  | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> |  | Checks made by usual daily testing of MSAW (every morning).<br><br><i>More frequent system checks?</i>   |
| <b>Missed alert</b>     |  |   |   |  |  |
| 2.                      | MSAW alert not generated due to <b>errors in DTED data</b>                             | The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin due to wrong, corrupted or erroneously computed DTED data.  | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | 1. Visualisation/Checking of source data against other DTED sources.<br><br>2. Visualisation/Checking of data that has been loaded into the system. Testing of MSAW (specifically, recording MSAW alerts and compare with MSAW model).   |
| 3.                      | MSAW alert not generated due to <b>undetected technical failure on the ground side</b> | The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin due to due to a tracking error, a coding problem or a hardware failure on the ground side (including RDPS, SNET, FDPS, etc.). | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | 1. Checks made by usual daily testing of MSAW (every morning).<br><br>2. Other mitigation methods recognised, including software development processes, testing and validation processes (incl. use of MSAW model for verification), routine monitoring of MSAW alerts (incl. comparing against MSAW model).<br><br>3. Tracker tuning, and demand that manufacturers fix identifiable shortcomings in the tracker. |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID: | Hazard Title   | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means  |
|------------|--|---|---|--|---|
| 4.         | MSAW alert not generated due to <b>undetected technical failure on the airborne side</b> | The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin due to a malfunctioning to airborne equipment (transponder, altimeter, pressure sensor, etc...) | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | Support programs for identifying and fixing faulty or “out of spec” transponders.   |
| 5.         | MSAW alert not generated due to <b>undetected erroneous QNH input</b>                    | The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin due to erroneous QNH value input in the RDPS (by Meteo Operator or automatic system)            | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | 1. Manual checking process.<br><br>2. Automatic detection of large jumps in QNH or unlikely QNH values (QNH can be back-computed by observing the FL on a/c touchdown). |
| 6.         | MSAW alert not generated due to <b>erroneous VFR/MIL code assigned</b>                   | The MSAW does not trigger an alert for an IFR flight infringing or about to infringe the vertical margin because a VFR/MIL code not eligible for MSAW has been erroneously assigned by the ATCO.  | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | Partially mitigated by the track representation (track correlation will be wrong and therefore detectable by the controller).   |
| 7.         | MSAW alert not generated due to <b>erroneous VFR/MIL code selected</b>                   | The MSAW does not trigger an alert for an IFR flight predicted to infringe the vertical margin because a VFR/MIL code not eligible for MSAW has been erroneously selected by the pilot.           | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of some potential risks of CFIT and there may be a proportionate increase in the number of CFIT prevented only by pilots to non MSAW levels</i> | <b>Severity 3</b>  | Partially mitigated by the track representation (track correlation will be wrong and therefore detectable by the controller).   |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID: | Hazard Title   | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means   |
|------------|--|---|---|--|--|
| 8.         | Missed MSAW alert due to <b>total loss of transponder function</b>                 | <p>The MSAW does not trigger an alert for an a/c predicted to infringe the vertical margin because the MSAW processes an outdated altitude higher than the actual one.</p> <p><i>(Note that in case of total transponder loss and in case of primary coverage available, the primary track takes over the track label together with the last altitude report attached. The correlation remains. The altitude report is kept at the last value for some time (10-30 sec) and then quietly disappears. As long as the altitude information is attached to the primary track by the RDPS the MSAW is available, but based on possibly incorrect altitude information).</i></p> | <p>ATM Safety not enhanced by MSAW</p> <p><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i></p> | <b>Severity 3</b>  | <p><i>Total loss of transponder introduces many other hazards, which are beyond the scope of this study.</i></p>   |
| 9.         | Missed MSAW alert due to <b>loss of transponder's altitude reporting component</b> | <p>The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin because a failure at the mode C set up causes the MSAW to process an outdated altitude higher than the actual one.</p>   | <p>ATM Safety not enhanced by MSAW</p> <p><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i></p> | <b>Severity 3</b>  | <p><u>Mode C age test</u></p> <p><i>MSAW to take age of height information into account. E.g. don't use data more than n seconds old.</i></p> <p><i>Loss of altitude reporting introduces many other hazards, which are beyond the scope of this study.</i></p>    |
| 10.        | MSAW alert not generated due to <b>erroneous inhibition</b> undetected by ATCO     | <p>An MSAW alert is not generated for an a/c infringing or about to infringe the vertical margin, because the track has been erroneously inhibited from alerting and the ATCO does not realize it, although the altitude indicated in red on the HMI</p>  | <p>ATM Safety not enhanced by MSAW</p> <p><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i></p> | <b>Severity 4</b>  | <p>1. Improve presentation of <b>DISABLED TRACKS</b>.</p> <p><i>(Note that the currently existing feature to show that the track has been inhibited from MSAW computing is the altitude displayed in red – see Figure 2-1).</i></p> <p>2. Controller Training.</p> |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID: | Hazard Title   | Hazard Description   | Hazard Effect on ATM   | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means  |
|------------|--|--|--|--|---|
| 11.        | MSAW alert not generated due to <b>premature inhibition</b> of MSAW  | An MSAW alert is not generated for an a/c infringing or about to infringe the vertical margin because the ATCO has inhibited the track as soon as the pilot has asked a visual approach departure and not after having issued the clearance for the visual departure, as required by the procedure.  | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i> | <b>Severity 4</b>  | 1. <i>Improve presentation of DISABLED TRACKS.</i><br>2. Controller Training.   |
| 12.        | MSAW alert not generated due to <b>MSAW not re-enabled</b> after acknowledgement procedure   | An MSAW alert is not generated for an a/c infringing or about to infringe the vertical margin because, after a previous acknowledgement procedure, the ATCO has forgotten to re-enable the track in a an evolved operational situation requiring the MSAW coverage<br><br><i>(e.g. an IFR flight which has previously asked a visual approach departure and then proceeds towards the Alps).</i>                         | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i> | <b>Severity 4</b>  | 1. <i>Improve presentation of DISABLED TRACKS.</i><br><i>Audible warning when track is DISABLED?</i><br>2. Controller Training. |
| 13.        | MSAW alert not generated due to <b>MSAW not re-enabled</b> after acknowledgement procedure by ATCO desensitized to acknowledgment procedure during transition to new MSAW<br><br>→ DELTA 2 | An MSAW alert is not generated for an a/c infringing or about to infringe the vertical margin because the ATCO has forgotten to re-enable a previously inhibited track, as s/he is less used to the acknowledgment procedure than with the previous MSAW system. With the new MSAW there is less pressure on ATCOs to suppress unnecessary alerts, due to the improved alerting performance of the DTED based algorithm. | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i> | <b>Severity 5</b>  | 1. <i>Improve presentation of DISABLED TRACKS.</i><br><i>Audible warning when track is DISABLED?</i><br>2. Controller Training. |
| 14.        | Missed MSAW alert due to <b>APM processing</b> taking priority<br><br>→ DELTA 2  | The MSAW does not trigger an alert for an a/c infringing or about to infringe the vertical margin because the APM processing takes priority over the MSAW (according to design requirements), although the a/c is not genuinely landing.   | ATM Safety not enhanced by MSAW<br><br><i>The Controller may not become aware of a potential risk of CFIT or may become aware too late for a corrective action to be performed</i> | <b>Severity 4</b>  | Testing using specific “worst case” test scenarios.   |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID:              | Hazard Title  | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means   |
|-------------------------|---|---|---|--|--|
| <b>Incomplete alert</b> |   |   |   |  |  |
| 15.                     | <b>MSAW visual alert not delivered</b>                              | The MSAW triggers the audible alert "Altitude, altitude" for an a/c predicted to infringe the vertical margin. Nevertheless there is no visual indication on the situation display of which aircraft is subject to the alert. | ATM Safety not enhanced by MSAW<br><i>Increased controller's workload due to the required scanning (or to the impossibility) to identify the implicated aircraft. Reduction of the ability to cope with other adverse operational and environmental conditions.</i> | <b>Severity 3</b>  | 1. Checks made by usual daily testing of MSAW (every morning).<br><br>2. Intense testing of MSAW function, in a variety of situations/configurations.  |
| 16.                     | <b>MSAW audible alert not delivered</b>                             | The MSAW triggers a visual alert for an a/c predicted to infringe the vertical margin. The visual indication, however, is not accompanied by the audible annunciation "Altitude, altitude".                                   | ATM Safety not enhanced by MSAW<br><i>Possible miss/late detection of the alert by ATCO for a corrective action to be performed (problem especially for TWR controllers)</i>  | <b>Severity 5</b>  | 1. Checks made by usual daily testing of MSAW (every morning).<br><br>2. <i>Dual audible chain? (already implemented, or possible to implement?).</i>  |
| <b>Delayed Alert</b>    |   |   |   |  |  |
| 17.                     | Delayed MSAW alert due <b>technical failure</b>                     | The MSAW triggers too late an alert for an a/c infringing or about to infringe the vertical margin due to a technical failure   | ATM Safety not enhanced by MSAW<br><i>Slight reduction of controller's capability to detect a potential risk of CFIT in a timely manner of for a corrective action to be performed</i>  | <b>Severity 4</b>  | <i>Recognised mitigation methods, including software development processes, testing and validation processes (incl. use of MSAW model for verification), routine monitoring of MSAW alerts (incl. comparing against MSAW model).</i> |
| 18.                     | Delayed MSAW due to <b>erroneous QNH input</b>                      | The MSAW triggers too late an alert for an a/c infringing or about to infringe the vertical margin because the QNH value input in the RDPS is lower than the actual one (input by Meteo Operator or automatic system).        | ATM Safety not enhanced by MSAW<br><i>Reduced controller's capability of becoming aware in a timely manner of a potential risk of CFIT for a corrective action to be performed</i>  | <b>Severity 3</b>  | 1. Manual checking process.<br><br>2. Automatic detection of large jumps in QNH or unlikely QNH values (QNH can be back-computed by observing the FL on a/c touchdown).  |
| 19.                     | Delayed MSAW alert due to late detection of <b>sudden manoeuvre</b> | The sudden manoeuvre of an a/c which is about to infringe the vertical margin causes a late detection by the tracker, leading the MSAW to trigger an alert too late for the situation to be solved                            | ATM Safety not enhanced by MSAW<br><i>Slight reduction of controller's capability to detect a potential risk of CFIT in a timely manner for a corrective action to be performed</i>   | <b>Severity 4</b>  | <i>Track tuning.</i>   |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID:                              | Hazard Title  | Hazard Description  | Hazard Effect on ATM   | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means  |
|---|---|---|--|--|---|
| 20.                                     | Delayed MSAW alert due to a/c proceeding towards <b>foot of steep mountain</b>                                    | The MSAW triggers too late an alert for the situation to be solved, because the a/c which is about to infringe the vertical margin is proceeding towards the foot of a very steep mountain. <i>(design requirement)</i>   | ATM Safety not enhanced by MSAW<br><br><i>Slight reduction of controller's capability to detect a potential risk of CFIT in a timely manner for a corrective action to be performed</i>  | <b>Severity 4</b>  | 1. Use of level off, and climb out predictions in MSAW.<br><br>2. Consider surrounding terrain as contributing to each cell of the loaded Digital Terrain grid. |
| <b>Incorrect addressing of alert</b>    |   |   |  |  |   |
| 21.                                     | MSAW alerts not delivered to the concerned CWP's due to <b>late or missing assumption of a/c</b><br><br>→ DELTA 2 | An MSAW alert for an a/c coming from a neighbouring ATC unit and predicted to infringe the vertical margin is not triggered on the concerned CWP's, because the ATCO in contact with the a/c has not yet assumed it. The alert is actually received by the transferring unit. | ATM Safety not enhanced by MSAW<br><br><i>Slight reduction of controller's capability to detect a potential risk of CFIT in a timely manner for a corrective action to be performed</i>  | <b>Severity 4</b>  | Thorough Testing of addressing mechanism.   |
| <b>Alert combined with other alerts</b> |   |   |  |  |   |
| 22.                                     | MSAW alert not noticed by TOWER ATCO due to <b>overlapping with other alerts/indications</b>                      | A TWR ATCO does not notice an alert pertaining to an a/c below the vertical margin because s/he is distracted by other simultaneous alerts and sound indications.<br><br>(e.g. note that the MSAW has currently the same voice of the STCA audible alert).                    | ATM Safety not enhanced by MSAW  | <b>Severity 3</b>  | <i>Use different voices for different types of alert, to help controllers to distinguish between them.</i><br><br>Controller Training.                          |
| 23.                                     | Activation of two <b>simultaneous MSAW alerts</b>   | An ATCO does not notice or is unable to timely manage an MSAW alert for an a/c infringing or about to infringe the vertical margin due to the simultaneous activation of another MSAW alert   | ATM Safety not enhanced by MSAW<br><br><i>Controller's workload increased through assessing which is the alert with higher priority, with reduced ability to detect a potential risk of CFIT in a timely manner for performing a corrective action</i> | <b>Severity 4</b>  | 1. HMI to help controller decide relative urgency of each alert (display alert severity or time to violation in track label?).<br><br>2. Controller training    |



EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard ID: | Hazard Title  | Hazard Description  | Hazard Effect on ATM   | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means   |
|------------|---|---|--|--|--|
| 24.        | Activation of an MSAW alert in <b>combination with an STCA alert</b>  | An ATCO does not notice or is unable to timely manage an MSAW alert for an a/c infringing or about to infringe the vertical margin due to the simultaneous activation of an STCA alert<br><br><i>(note that the STCA alert could involve the same track or another track)</i>   | ATM Safety not enhanced by MSAW<br><br><i>Controller's workload increased through assessing which is the alert with higher priority, with reduced ability to detect a potential separation infringement or a potential risk of CFIT in a timely manner for performing a corrective action</i>              | <b>Severity 4</b>  | <ol style="list-style-type: none"> <li>1. HMI to help controller decide relative urgency of each alert</li> <li>2. Controller training.</li> <li>3. When the alerts concern different tracks should airborne side logic be emulated on the ground side? – i.e. MSAW always takes priority over STCA).</li> </ol> |
| 25.        | Activation of an MSAW alert in <b>combination with an APW alert</b>   | An ATCO does not notice or is unable to timely manage an MSAW alert for an a/c infringing or about to infringe the vertical margin due to the simultaneous activation of an APW alert<br><br><i>(Note that the APW alert could involve the same track or another track)</i><br><br><i>(Note the he hazard is formulated assuming that an APW will be implemented in Skyguide)</i> | ATM Safety not enhanced by MSAW<br><br><i>Controller's workload increased through assessing which is the alert with higher priority, with reduced ability to detect a potential infringement of a protected airspace or a potential risk of CFIT in a timely manner for performing a corrective action</i> | Severity 4   | <ol style="list-style-type: none"> <li>1. HMI to help controller decide relative urgency of each alert</li> <li>2. Controller training.</li> <li>3. When the alerts concern different tracks should MSAW always takes priority over APW?</li> </ol>  |
| 26.        | Activation of an MSAW alert in <b>combination with a RIMCAS alert</b> | An ATCO does not notice or is unable to timely manage an MSAW alert for an a/c infringing the vertical margin due to the simultaneous activation of a RIMCAS alert<br><br><i>(Note that the RIMCAS alert could involve the same track or another track)</i>   | ATM Safety not enhanced by MSAW<br><br><i>Controller's workload increased through assessing which is the alert with higher priority, with reduced ability to detect a potential risk of runway incursion or a potential risk of CFIT in a timely manner for performing a corrective action</i>             | <b>Severity 4</b>  | <ol style="list-style-type: none"> <li>1. HMI to help controller decide relative urgency of each alert?</li> <li>2. Controller training.</li> </ol>  |

**MSAW FHA – NEGATIVE EFFECT ON SAFETY**

| Hazard Ref:             | Hazard Title  | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means   |
|-------------------------|---|---|---|--|--|
| <b>Loss of function</b> |   |   |   |  |  |
| 27.                     | <b>Undetected total loss of MSAW</b>                                  | ATCOs are not aware the MSAW will not trigger any alert in case of a/c infringing or about to infringe the vertical margin in all the MSAW coverage area  | Negative effects on ATM safety  | <b>Severity 3</b>  | Checks made by usual daily testing of MSAW (every morning).<br><br><i>More frequent system checks?</i>   |
| 28.                     | <b>Total loss of MSAW erroneously indicated as operational on CWP</b> | ATCOs are not aware the MSAW will not trigger any alert in case of a/c infringing or about to infringe the vertical margin in all the MSAW coverage area, although the MSAW is erroneously indicated as being operational on CWP and supervisor working position. | Negative effects on ATM safety  | <b>Severity 3</b>  |  |
| <b>Nuisance alert</b>   |   |   |   |  |  |
| 29.                     | Nuisance MSAW alert due to <b>errors in DTED data</b>                 | The MSAW triggers an undesirable alert for an a/c not infringing nor predicted to infringe the vertical margin due to wrong, corrupted or erroneously computed DTED data.   | Negative effects on ATM safety<br><br><i>The Controller's workload increased through assessing Alerts for validity. If the problem occurs with more tracks it may distract the Controller to the point that there may be a proportionate increase in the number of conflicts and potential risks of CFIT higher than non MSAW levels.</i> | <b>Severity 3</b>  | 1. <i>Visualisation/Checking of source data against other DTED sources.</i><br><br>2. <i>Visualisation/Checking of data that has been loaded into the system. Testing of MSAW (specifically, recording MSAW alerts and compare with MSAW model).</i> |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard Ref: | Hazard Title  | Hazard Description   | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means  |
|-------------|---|--|---|--|---|
| 30.         | Nuisance MSAW alert due to <b>erroneous QNH input</b>   | The MSAW triggers an undesirable alert for an a/c not infringing nor predicted to infringe the vertical margin because the QNH value input in the RDPS (by Meteo Operator or automatic system) is higher than the real one.  | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. If the problem occurs with more tracks it may distract the Controller to the point that there may be a proportionate increase in the number of conflicts and potential risks of CFIT higher than non MSAW levels.</i> | <b>Severity 5</b>  | 1. Manual checking process.<br><br>2. Automatic detection of large jumps in QNH or unlikely QNH values (QNH can be back-computed by observing the FL on a/c touchdown). |
| 31.         | Nuisance MSAW alert due <b>total loss or loss of altitude reporting component of transponder function</b> | The MSAW triggers an undesirable alert for an a/c not infringing nor predicted to infringe the vertical margin because the MSAW processes an outdated altitude lower than the actual one.<br><br><i>(Note that in case of total transponder loss and in case of primary coverage available, the primary track takes over the track label together with the last altitude report attached. The correlation remains. The altitude report is kept at the last value for some time (10-30 sec) and then quietly disappears. As long as the altitude information is attached to the primary track by the RDPS the MSAW is available, but based on possibly incorrect altitude information).</i> | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. This causes a slight reduction of the ability to cope with adverse operational and environmental conditions.</i>  | <b>Severity 4</b>  | <u>Mode C age test</u><br><br><i>MSAW to take age of height information into account. E.g. don't use data more than n seconds old.</i>                                  |
| 32.         | Nuisance MSAW alert due to <b>technical failure on the ground side</b>                                    | The MSAW triggers an undesirable alert for an a/c not infringing nor predicted to infringe the vertical margin, due to a tracking error, a coding problem or a hardware failure on the ground side (including RDPS, SNET, FDPS, etc.)  | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. This causes a slight reduction of the ability to cope with adverse operational and environmental conditions.</i>  | <b>Severity 4</b>  | 3. Tracker tuning, and demand that manufacturers fix identifiable shortcomings in the tracker.  |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard Ref:                 | Hazard Title  | Hazard Description  | Hazard Effect on ATM  | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means  |
|-----------------------------|---|---|---|--|---|
| 33.                         | Nuisance MSAW alert due to <b>technical failure on the airborne side</b>                              | The MSAW triggers an undesirable alert for an a/c not infringing nor predicted to infringe the vertical margin, due to a malfunctioning to airborne equipment (transponder, altimeter, pressure sensor, etc.)   | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. This causes a slight reduction of the ability to cope with adverse operational and environmental conditions.</i>  | <b>Severity 5</b>  | Support programs for identifying and fixing faulty or "out of spec" transponders.   |
| 34.                         | Nuisance MSAW alert due to <b>IFR code erroneously assigned</b> to VFR/MIL flight                     | The MSAW triggers an undesirable alert to a VFR/MIL aircraft below or about to infringe the vertical margin because an IFR code has been erroneously assigned to it   | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. This causes a slight reduction of the ability to cope with adverse operational and environmental conditions.</i>  | <b>Severity 5</b>  | Partially mitigated by the track representation (track correlation will be wrong and therefore detectable by the controller). |
| 35.                         | Nuisance MSAW alert due to <b>IFR code erroneously selected</b> by VFR/MIL flight                     | The MSAW triggers an undesirable alert for a VFR/MIL aircraft below or about to infringe the vertical margin because an IFR code has been erroneously assigned to it  | Negative effects on ATM safety<br><br><i>Controller's workload increased through assessing Alerts for validity. This causes a slight reduction of the ability to cope with adverse operational and environmental conditions.</i>  | <b>Severity 5</b>  |   |
| <b>Incorrect addressing</b> |   |   |   |  |   |
| 36.                         | MSAW alert sent to all CWP's due to <b>late or missing assumption</b> of a/c by ATCO<br><br>→ DELTA 2 | An MSAW alert is activated for an a/c predicted to infringe (or infringing) the vertical margin also on the CWP's of ATCOs who are not in contact with it (including TWR, ARR/DEP/FIN/APC CWP's), because the concerned ATCO has not yet assumed the a/c as required. | Negative effects on ATM safety<br><br><i>In the short term, controller's workload increased through assessing Alerts for validity, with slight reduction of the ability to cope with adverse operational and environmental conditions.</i><br><br><i>In the medium-long term, controller desensitized to genuine alerts, with reduced capability of becoming aware in a timely manner of a potential risk of CFIT</i> | <b>Severity 3</b>  | 1. Improve presentation of DISABLED TRACKS.<br><br>2. Controller Training.  |

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning  
Appendix D-2: Functional Hazard Assessment of MSAW for Skyguide

| Hazard Ref: | Hazard Title   | Hazard Description  | Hazard Effect on ATM   | Severity & Exposure Time<br>(Ref SAM Severity Classification Scheme) | Mitigation Means                          |
|-------------|--|---|--|--|---|
| 37.         | MSAW alert sent to CWP for which it is not relevant due to <b>technical failure in the addressing mechanism</b><br><br>→ DELTA 2 | An MSAW alert is activated for an a/c predicted to infringe (or infringing) the vertical margin also on the CWPs of ATCOs who are not in contact with it (including TWR, ARR/DEP/FIN/APC CWPs), because the concerned ATCO has not yet assumed the a/c as required. | Negative effects on ATM safety<br><br><i>In the short term, controller's workload increased through assessing Alerts for validity, with slight reduction of the ability to cope with adverse operational and environmental conditions.</i><br><br><i>In the medium-long term, controller desensitized to genuine alerts, with reduced capability of becoming aware in a timely manner of a potential risk of CFIT.</i> | <b>Severity 3</b>  | Thorough Testing of addressing mechanism. |

## 6. CONCLUSIONS

The FHA study has produced two different kinds of results:

- An input for the completion of an overall MSAW safety case in compliance with ESARR 4 requirements
- A feedback – from a safety point of view – on the design solutions and recommendations proposed in the associated Appendix D1 (Enhancement of MSAW for Skyguide).

### 6.1 Input for an MSAW Safety Case

The first result consists of a list of identified hazards and in the classification of the severity of their effects, to be considered for establishing an adequate set of *safety objectives*.

This part of the work has been complemented by proposing a list of possible mitigation means - including technical, procedural and training solutions- to both reduce the severity and the frequency of the effects associated to each hazard. Although such list is still provisional and the solutions require further study for their actual implementation in Skyguide, a relevant input has been provided for the identification of a specific set of *safety requirements* to be used in the design phase at a PSSA level (Preliminary System Safety Assessment).

### 6.2 Safety Feedback to MSAW Enhancement Recommendations

The FHA study has confirmed the validity of the recommendations provided by the MSAW enhancement study with respect to the four key issues addressed in the case study:

- The changes required for MSAW coverage scalability.
- The choice between hand designed polygons and DTED.
- The choice between detection and prediction.
- The adequacy of aircraft eligibility criteria.

The majority of hazards identified do not challenge the design solutions suggested in the study and can be mitigated by technical means and procedures not altering the fundamental design choices of the envisaged MSAW system.

The FHA analysis, however, revealed also a few cases in which further study is required to make sure that the adopted design will not cause a too limited benefit for safety or even a negative effect on it.

In the following subsections these open issues are briefly analyzed.

### **6.2.1 Undesired Side Effects of the Addressing Mechanism**

The FHA analysis highlighted a potential side effect of the MSAW alert addressing mechanism, once the MSAW geographical coverage will be extended to the whole Skyguide Area of Responsibility. On one hand the new proposed system will make the MSAW protection available at a wider range of CWPs, including TWR, ARR, DEP, FIN, APC. On the other hand the addressing mechanism will let the MSAW send the audible and visual alert only to the controller who has actually assumed the track causing the alert. Such mechanism guarantees that no nuisance alerts are addressed to the CWPs not interested by any potential risk of CFIT.

During the FHA workshop, however, it was argued that in the event of a late or missing assumption of the track by the concerned ATCO, the alert will be sent to all CWPs, causing considerable disturbance in the control room, particularly for controllers who don't have the aircraft in sight, but still receive the audible alert. Such effect could obviously be determined also in case of technical failure of the addressing mechanism itself (see hazards 36 and 37 in the FHA table).

Although the frequency of these hazards is expected to be low, the potential negative impact on safety requires further study to make sure that the adopted addressing mechanism is the best option for the future MSAW system and which additional technical features can be identified to minimize the severity of the expected safety impact.

### **6.2.2 Combination of MSAW alerts with other alerts**

From an operational point of view the activation of more alerts at the same time is always considered a highly undesirable event to be minimized as far as reasonably possible. Although the combined activation of an MSAW with another MSAW or with other ground based safety nets, such as STCA, APW or RIMCAS is considered a rare event, the operational representatives in the FHA workshop have argued that this risk could potentially be increased by the extension of MSAW availability to a wider number of CWPs (see hazards 22-23-23-25-26 in the FHA table). A special concern has been raised with respect to TWR positions, where controllers are often subjects to a very intense workload and the combined activation of different alerts can more easily jeopardize the efficacy their performance<sup>3</sup>.

---

<sup>3</sup> It is worth noting that, the combined activation of MSAW with other ground based safety nets (STCA, APW, RIMCAS) could pertain to the same a/c triggering the MSAW alert or to another a/c, thus increasing the number of possible combinations.

It is then recommendable that the extension of MSAW to a wider geographical area and number of CWPs will be accompanied by a careful consideration of these potential interactions. In other words the expected safety benefit gathered by the increased MSAW protections should be compared against the potential detriment caused by controllers experiencing difficulties in managing multiple alerts.

With respect to the specific case of TWR controllers, a special attention should be devoted to the design of MSAW inhibitions area in the vicinity of airports and, when available, to the interfacing with Aircraft Path Monitoring (APM) funnels.

### **6.2.3 Terrain collision geometries potentially challenging the DTED performance**

The MSAW enhancement case study has shown that the DTED based logic performs considerably better than manually designed polygons, as the former clearly provides a better trade off between nuisance alerts and anticipated warning time. Nevertheless, during the FHA workshop, two extreme scenarios of terrain collision geometries were discussed that could potentially challenge the effectiveness of the more refined DTED grid in providing a timely MSAW alert (see hazards 19 and 20 in the FHA table).

The first scenario concerned an aircraft performing a sudden manoeuvre in the lateral plan which causes the track to head towards a huge obstacle or mountain which was previously not in its trajectory. In such extreme scenario the tracker could potentially detect too late the new trajectory of the aircraft for providing a timely MSAW alert to the controller.

The second scenario concerned an aircraft proceeding towards the foot of a very steep mountain. In such geometry, although the DTED logic is of course able to trigger an MSAW alert 45 seconds before the infringement of the vertical margin, there is a risk that an evasive manoeuvre required by the ATCO will anyhow result ineffective for the pilot to timely react.

Although both scenarios seem to refer to extremely unlike situations for controlled aircraft, it was argued that further reflections should be made to understand whether additional design features could help in minimizing such risks, whilst keeping all the advantages of the DTED logic in the large majority of situations (see the proposed mitigation means to hazards 19 and 20).



END OF DOCUMENT