KURDISTAN REGIONAL GOVERNMENT

SULAYMANIYAH INTERNATIONAL AIRPORT

MATS

APPENDIX " K "

RISK ASSESSMENT OF ATS PROCEDURES

(First Edition)

April 2012

Prepared By
Fakhir .F. Mohammed
Civil Aviation Consultant

Appendix " K "
RISK ASSESSMENT OF ATS PROCEDURES

1. PURPOSE

1.1 The objective of assessing ATS procedures is to ensure that, as far as reasonably practicable, potential hazards associated with the control of aircraft have been identified and actions to mitigate the associated risks have been put in place.

1.2 This appendix provides general guidance on hazard identification and risk assessment processes that are useful in the development or modification of ATS procedures.

2. HAZARD IDENTIFICATION (HAZid)

2.1 HAZid is a relatively thorough "top-down" technique that breaks down activities associated with the implementation of ATS procedures into smaller components and identifies their potential failure modes and their effect on ATS safety. Specifically, the HAZid technique is used to identify:

a. ATS - Related Hazards: A hazard is defined as a source of potential harm or a situation with a potential to cause loss. Basic ATS-related hazards include:

1. mid-air collisions;

2. collisions on the ground;

3. wake vortex encounters;

4. turbulence events; and

5. collisions with the ground.

b. Hazardous Scenarios: Hazardous scenarios describe the specific hazard under consideration. For example, when considering the mid-air collision hazard at an airport, hazardous scenarios might be:

1. **a mid-air collision between a departing and an arriving aircraft; and**

2. **a mid-air collision between aircraft on parallel approach.**

c. **Initiating Events: The initiating events describe the generic reasons for the hazardous scenario occurring. This may be a deviation from a flight path. For example, various initiating events for the hazardous scenarios of a mid-air collision between a departing and an arriving aircraft include an aircraft busting a level restriction, or an aircraft deviating from a SID or STAR.**

d. **Hazard Causes: The hazard causes describe how the initiating event started. Initiating events may be caused by external influences, human error, equipment failure or procedure design mistakes that can start a chain of events which could lead to a hazard. For an aircraft deviating from a SID, the cause could be an equipment failure such as a control system failure, or human error such as a pilot selecting the wrong SID in the flight management system (FMS).**

e. **Recovery Factors: The recovery factors describe the systems available to prevent or reduce the likelihood of initiating events becoming hazardous scenarios. For a mid - air collision, the recovery factors include the provision of ATC, the use of TCAS, pilot "see and avoid", and the flight path geometry.**

f. **Recovery Factor Failures: Recovery factors might fail to prevent a mid-air collision. Recovery factor failures for TCAS could include a transponder not being fitted to one of the aircraft, or the pilot not reacting to the alerts.**

2.2 The HAZid method uses keywords or prompt words to systematically generate possible deviations from the norm for ATS and flying tasks. The procedure then examines the effect of each deviation on ATS-related safety.

2.3 External Influences

HAZid begins by considering the external influences on a single aircraft on a fixed flight path. The sources of these external influences could be, for example:

a. meteorological;

b. topographical;

c. environmental; and

d. man-made.

2.4 Possible Deviations From Planned Flight Path

Once external influences to safe flight are identified and recorded, the HAZid technique considers possible deviations from the planned flight path and how these may be caused by internal operational events. These deviations may become initiating events for hazardous scenarios. Typical sources of internal operational events include:

a. ATC separation;

b. navigation aids;

c. airport design — runway;

d. airspace design;

e. aircraft design and maintenance; and

f. aircraft operation.

2.5 Keywords or prompt words are used to systematically identify possible deviations from planned flight paths. Possible deviations are examined through a "bottom-up" consideration of:

a. **Procedures In Use: The procedures in use relate to the design of airspace and airports, ATC procedures and flight procedures. These procedures can lead to hazardous scenarios without additional system failures, i.e. hazardous scenarios can exist without requiring deviations from normal flight paths. For example, the vertical separation buffer for the base of CTA can be 500 ft.**
However, wake turbulence separation is applied when an aircraft is operating up to 1 000 ft below.

b. **Human tasks: Human tasks may fail through various types of human error. This is a specialist area of analysis, and advice should be sought from appropriate Human Factors specialists.**

c. **Equipment Functionality: A failure modes and effects analysis (FMEA) is normally used to analyze the influences of equipment failures on the ATS system. The method is applied at the functional level to all ATS equipment, aircraft communication equipment, and navigation, surveillance, flight control and power plant equipment.**

d. **Geometric Factors: There may be other factors that are not related to human error or equipment failure but are still necessary for the hazard to occur. This is usually a description of the geometry of encounter.**

3. HAZARD ANALYSIS

3.1 Having identified particular hazards, several techniques are available for assessing them, both qualitatively and quantitatively. Some techniques require specialist expertise in their application. Typically, the hazard analysis process involves:

a. development of fault schedules;

b. construction of fault trees; and

c. quantification of the likelihood of human error, equipment failure and operational factors.

3.2 Fault Schedules

3.2.1 Fault schedules are used to record the results of the HAZid process for each hazardous scenario. An example of a hazardous scenario might be a mid-air collision between an arriving and a departing aircraft when the arriving aircraft fails to intercept the localizer.

3.2.2 The initiating event for this scenario would be that the arriving aircraft heads into the flight path of the departing aircraft. The fault schedule would record possible causes for the initiating event, including airborne or ground equipment faults, and human error by either the pilot or ATC (for example, call sign confusion). Recovery factors include existing or missing defences designed to reduce the likelihood of the initiating event becoming a hazardous scenario. Each recovery factor is examined as to why it failed to prevent the situation from developing.

3.3 Fault Trees

3.3.1 Information contained in the fault schedules may be used to construct a fault tree. The level of analysis for the fault tree will depend on the situation. However, as a general guide, a simple pessimistic model should be used initially to determine the likelihood of human error, equipment failure and operational factors and thus the operational risk exposure. This risk exposure is then compared with the risk criteria for the target level of safety. If the pessimistic model produces a result that is lower than the target criteria, then further resource allocation is not required as it would not alter the risk management decision.

3.4 Consequence Analysis

3.4.1 The amount of loss for ATS-related risk assessments is normally measured as the number of fatalities that would result from the most drastic possible outcome. For example, a simple analysis of mid-air collisions and collisions with the ground assumes that all people on board the aircraft will die as the result of a mid-air collision and most collisions with the ground.

4. RISK ASSESSMENT

4.1 As outlined in Doc 9859 Chapter 6, a key phase of risk management involves the assessment of identified risks. Formal risk assessments must be performed:

a. for significant changes to ATS procedures compared with current operations;

b. for significant changes to equipment used to execute ATS tasks compared with current operations; and

c. when changing circumstances, such as increased traffic levels, and different aircraft performance, indicate that existing procedures may not be appropriate.

4.2 Table Appendix " K ". ATS risk assessment procedures offers several steps for assessing risks inherent in hazards found in ATS procedures.

4.3 Risk Analysis

4.3.1 Risk is calculated as the product of the likelihood of a hazardous event and the consequences of the event happening. Risk analysis may be quantitative or qualitative depending on the risk information and data readily available, the magnitude of the hazard, and other factors. Use of quantitative data helps clarify most decisions and should be used where available; however, some of the most important factors in a decision can be impractical to quantify. (For example, often when examining people and procedures in the provision of a separation service, qualitative descriptions and comparison scales are all that are available.) Care should be taken to consider these factors also.

4.4 Risk Management

4.4.1 The principles and steps of risk management are outlined in Doc 9859 Chapter 6. Management must decide if:

a. the risk is so great that it must be refused altogether;

b. the risk is, or has been made, so small as to be insignificant (however, any actions that reduce risk and require little effort or resources must be implemented); or

c. the risk falls between the two states in (a) and (b) and has been reduced to the lowest level practicable, bearing in mind the benefits derived from its acceptance and taking into account the costs of any further reduction.

Table Appendix " K ". ATS risk assessment procedures

Step 1	**Identify whether the change involves a change in control procedure, in equipment, or in both**
Step 2	**Break down the procedures into manageable components,. For example, control procedures might be divided into :** **a. transfer of control procedures;** **b. coordination procedures;** **c. radar procedures;** **d. holding procedures;** **e. speed control procedures; and** **f. runway procedures** **Equipment user procedures might be divided into :** **a. set – up procedures;** **b. operations under normal and emergency conditions; and** **c. operations under equipment failure or partial failure conditions.**
Step 3	**Identify potential hazards that affect the ability to maintain safe separation. This is best achieved by asking " What can go wrong? " and " What if …. ? " in relation to the identified divisions in Step 2. It is necessary to consider the impact of the procedure on all levels of controller ability and experience.**
Step 4	**Identify the circumstances or incident sequence under which a hazard might occur, together with the likelihood of occurrence. Having considered the likelihood and consequences of occurrence, some identified hazards may be discounted as unrealistic. The reasons for discounting must be recorded.**
Step 5	**Make an assessment of the hazard severity.**
Step 6	**Examine the hazard and incident circumstances and identify essential and desirable measures that, when implemented, will mitigate or eliminate the hazard.**