Republika e Kosovës
Republika Kosovo - Republic of Kosovo

Autoriteti i Aviacionit Civil i Kosovës
Autoritet Civilnog Vazduhoplovstva Kosova
Civil Aviation Authority of Kosovo

Technical Publication – TP 12

Air Navigation System Safety Assessment Methodology-SAM

Guidance Material for the application of SAM

Foreword

The provision of air navigation services plays a central role in ensuring the safety of air traffic, since it provides the primary means of avoiding aircraft collisions. As such it is an intrinsically risky operation requiring a strict safety management system. Modern safety management practice rightly demands that before making a change to a safety related system appropriate steps are taken to ensure that the change does not introduce an unacceptable risk into the system.

Regulation 12/2009 issued by Civil Aviation Authority of Republic of Kosovo, which transposes EC Regulation 2096/2005 laying down common requirements for the provision of services, places responsibilities directly on Air Navigation Service Providers (ANSPs) regarding safety, and in particular they require ANSPs to perform risk assessment and mitigation in respect to changes to the ATM system.

This Guidance Material provides an introduction to the EUROCONTROL's Safety Assessment Methodology (SAM), which is considered to be one of Acceptable Means of Compliance with the Common Requirements regarding changes to ANS systems. This Guidance Material covers the SAM basics as well as offers guidance to ANSPs on how to address various changes and how to approach the risk assessment and mitigation process. Furthermore, this document is supplemented by three other Guidance Materials addressing the individual phases of SAM, namely CAAK TP-13 which addresses the Functional Hazard Identification (FHA), CAAK TP-14 which addresses Preliminary System Safety Assessment (PSSA) and CAAK TP-15 which addresses System Safety Assessment (SSA). Hence, this Guidance Material should be applied taking into consideration the complementary Guidance Materials available for SAM, as well as ANSPs' own Safety Management Manuals.

Furthermore, the content of this Guidance Material broadly addresses subject matter related to risk assessment and mitigation, therefore ANSPs should apply caution when using this material, since it is their responsibility to determine the exact requirements deriving from the Common Requirements and not simply refer to the guidance offered in this publication. ANSPs must also ensure that when used, this Guidance Material must be suitably adapted to the particular change.

Dritan Gjonbalaj
Director General
Civil Aviation Authority

List of Effective Pages

Chapter	Pages	Revision Nr.	Effective Date
Foreword	2 of 36	First Issue	23 June 2011
List of Effective Pages	3 of 36		23 June 2011
	4 of 36		23 June 2011
Table of Contents	5 of 36		23 June 2011
	6 of 36		23 June 2011
Terms and Definitions	7 of 36		23 June 2011
	8 of 36		23 June 2011
	9 of 36		23 June 2011
Chapter 1 - Introduction	10 of 36		23 June 2011
	11 of 36		23 June 2011
	12 of 36		23 June 2011
	13 of 36		23 June 2011
	14 of 36		23 June 2011
Chapter 2 – What is a “change”?	15 of 36		23 June 2011
	16 of 36		23 June 2011
	17 of 36		23 June 2011
	18 of 36		23 June 2011
	19 of 36		23 June 2011
	20 of 36		23 June 2011
	21 of 36		23 June 2011
Chapter 3 – Safety Planning	22 of 36		23 June 2011
	23 of 36		23 June 2011
	24 of 36		23 June 2011
	25 of 36		23 June 2011
	26 of 36		23 June 2011
Chapter 4 – The SAM Process	27 of 36		23 June 2011
	28 of 36		23 June 2011
	29 of 36		23 June 2011
	30 of 36		23 June 2011
	31 of 36		23 June 2011
	32 of 36		23 June 2011
	33 of 36		23 June 2011
	34 of 36		23 June 2011
Appendix A - Unexpected tactical change checklist	35 of 36		23 June 2011
	36 of 36		23 June 2011

	Name and position	Date	Signature
Prepared by:	**Zana Limani,** Officer, Air Navigation Services Department	10 May 2011	
Authorized by:	**Arianit Islami** Director, Air Navigation Services Department	12 May 2011	
Quality Check by:	**Lendita Kika-Berisha** Manager, Internal Auditing and Quality Management	21 June 2011	
Approved by:	**Dritan Gjonbalaj** Director General	23 June 2011	

Table of Contents

Terms and Definitions

Acceptable risk	Acceptable risk defines the target risk for an ANSP as defined in their Risk Classification Scheme (RCS).Acceptable risk is more demanding than tolerable risk.
ANS Air Navigation Service(s)	Air traffic services; communication, navigation and surveillance services; meteorological services for air navigation; and aeronautical information services.
ANSP	An 'Air navigation service provider' (ANSP) shall be understood to include an organisation having applied for a certificate to provide such services.
Assumption	Statement, principle and/or premises offered without proof.
ATM	The aggregation of ground based (comprising variously ATS, ASM, ATFM) and airborne functions required ensure the safe and efficient movement of aircraft during all appropriate phases of operations
ATM functional system	ATM functional system' shall mean a combination of systems, procedures and human resources organised to perform a function within the context of ATM;
ATM System	ATM System is a part of ANS System composed of a Ground Based ATM component and an airborne ATM component
EASA	European Aviation Safety Agency
EATMP	EUROCONTROL's European Air Traffic Management Programme
EC	European Commission

Environment of operations	The environment of operations consists of the physical and institutional characteristics of the airspace within which operations occur. The environment includes ATM services being provided, technologies used, airspace organisation, ambient conditions and people.
ESARR	EUROCONTROL Safety Regulatory Requirement
EU	European Union
EUROCAE	The European Organisation for Civil Aviation
Hazard	Any condition, event, or circumstance which could induce an accident.
Incident	An occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operations.
Mitigation (or risk mitigation)	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.
National Supervisory Authority (NSA)	The body or bodies nominated or established by EU Member States as their national authority pursuant to Article 4 of Regulation (EC) No. 549/2004.
Risk	The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.
Risk Assessment	Assessment to establish that the achieved or perceived risk is acceptable or tolerable
Safety	Freedom from unacceptable risk.
Safety Assurance	All planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a system achieves acceptable or

	tolerable safety
Safety Objective	Quantitative or qualitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur.
Safety Requirement	A risk mitigation means, defined from the risk mitigation strategy, that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.
Severity	Level of effect/consequences of hazards on the safety of operations, including the aircraft operations.
Severity Class	Gradation, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the effects of hazards on operations, including the aircraft operations.
Target Level of Safety	A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable or tolerable risk.
Tolerable risk	Tolerable risk defines the target risk for a National Regulator as defined in their Risk Classification Scheme (RCS).
Validation	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. (ISO 8402)
Verification	Confirmation by examination and provision of objective evidence that the requirements have been fulfilled. (ISO 8402)

Chapter 1

Introduction

1.1 Regulatory Requirements

1.1.1 CAAK Regulation 12/2009

According to Regulation 12/2009 which transposes EC Regulation 2096/2005 laying down the common requirements for the provision of air navigation services (ANS), Annex II Article 3.2, ANS Providers are required to ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to the ATM functional system. Furthermore, the results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures that complete arguments are established to demonstrate the overall ATM functional system is, and will remain tolerably safe by meeting allocated safety objectives and requirements.

1.2 Purpose and Scope

1.2.1 Purpose

The purpose of this guidance material is to provide an introduction to the EATMP's Safety Assessment Methodology (SAM), which is considered by CAAK to be one of the Acceptable Means of Compliance (AMC) for the requirements laid down in Annex II Article 3.2.1-3.2.4 of CAAK Regulation 12/2009.

SAM has been approved by EUROCONTROL to be an AMC for a substantial portion of ESARR 4 (Risk Assessment and Mitigation in ATM), which were adopted into European Community Law through EC Regulation 2096/2005 laying down common requirements for ANS Providers. The relationship between ESARRs issued by EUROCONTROL and EC Regulation in force is illustrated in Figure 1.

1.2.2 Scope

This guidance material covers the basis of SAM methodology, including steps that should be considered prior to initiating the SAM process itself (FHA, PSSA and SSA phases), such as identifying and classifying changes as well as planning safety activities.

Due to the extensive scope, the individual phases of SAM will be addressed in separate Guidance Materials, one for each: FHA, PSSA and SSA.

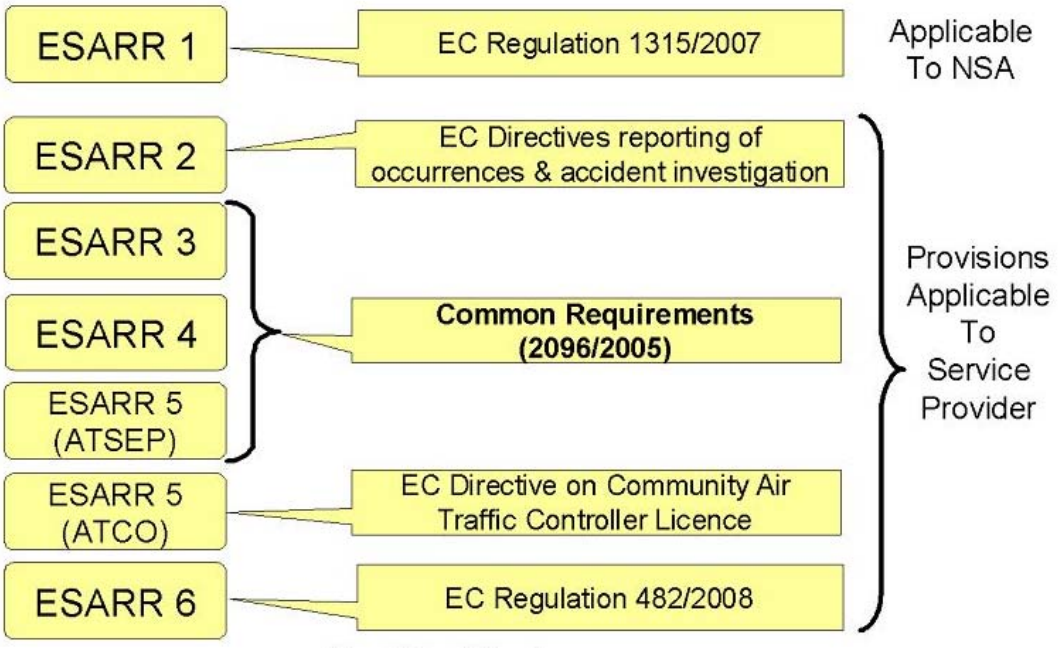

Figure 1 - Relationship between ESARRs and EC Legislation

1.3 What is SAM?

SAM is a methodology developed by EUROCONTROL's European Air Traffic Management Programme (EATMP) to reflect best practices for safety assessment of Air Navigation Systems and to provide guidance for their application.

SAM methodology describes a generic process for the safety assessment of Air Navigation Systems.

This process consists of three major steps as shown in the figure below:

- Functional Hazard Assessment (FHA);
- Preliminary System Safety Assessment (PSSA);
- System Safety Assessment (SSA).

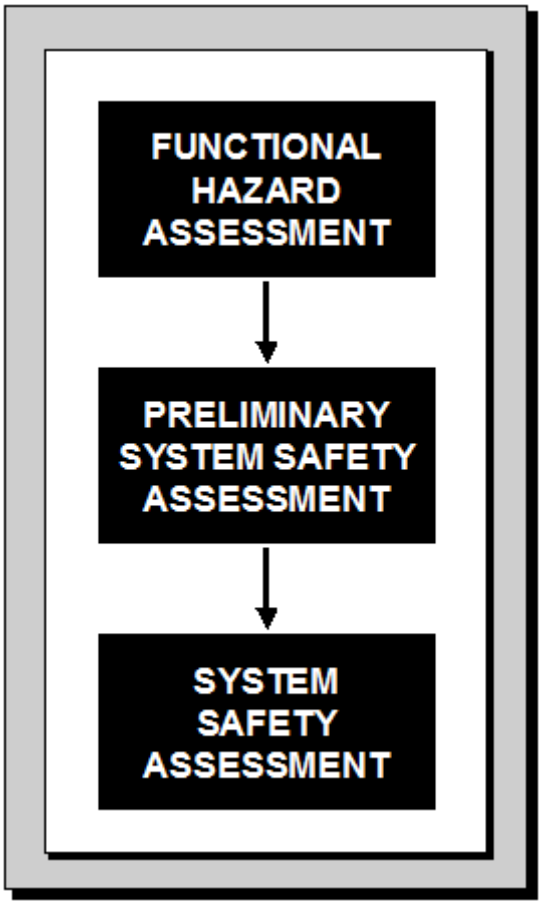

Figure 2 - The three phases of SAM

These steps are closely interlinked to the system's overall lifecycle phases. The relationship between them is shown in the figure below.

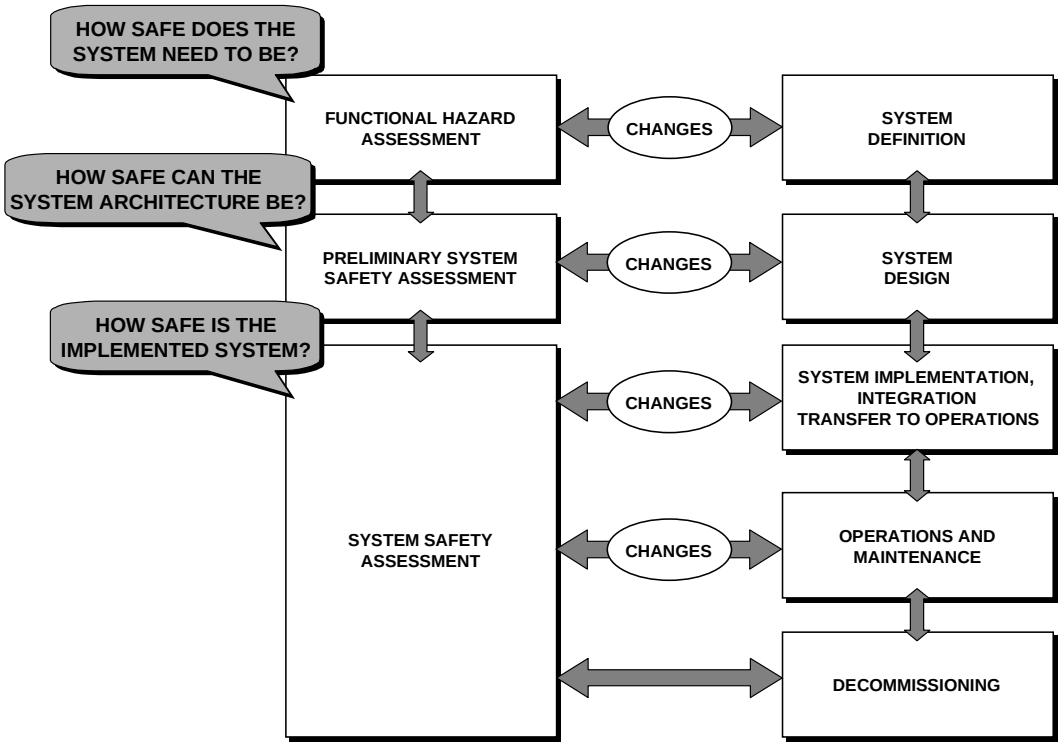

Figure 3 - Relationships between the Safety Assessment Process and the Overall System Life Cycle

SAM describes the underlying principles of the safety assessment process and leaves the details of applying these principles (or supplementing them if necessary) to be defined for each specific project.

SAM provides further guidance for developing the EATMP Safety Management Principles of the EATMP Safety Policy, in particular the following:

- Risk Management Process;
- Safety Objectives and Requirements;
- System Safety Assessment Process and Documentation.

SAM should potentially support the demonstration that safety is being managed within safety levels meeting as a minimum those approved by the CAAK ("tolerable" risk). However, SAM aims at supporting ANSP to achieve an acceptable level of risk. (See Terms and Definitions).

1.3.1 Scope of the methodology

An Air Navigation System may include ground-based (including space-based components) and air-based components. The methodology covers the complete life-cycle of the Air Navigation System, from initial planning and system definition to de-commissioning.

The methodology however, considers only the safety aspects of the Air Navigation System. Other attributes of the system, aiming, for example, to achieve capacity and/or efficiency objectives, are not addressed by the proposed methodology.

SAM provides guidelines on how to perform an Air Navigation System Safety Assessment. SAM methodology does not address Air Navigation System "certification" issues. However, the application of the principles described in this manual could prepare and support a certification process of Air Navigation Systems. (Cf. EUROCAE ED78A" Guidelines for approval of the provision and use of Air Traffic Services supported by data communication" may be used for approval purposes.)

SAM methodology does not address organisational and management aspects related to safety assessment. Acceptability of those changes should be assessed as part of the implementation of an organisation Safety Management System. For each project, organisational entities involved in the safety assessment process should be identified and their respective responsibilities specified.

SAM methodology also provides guidance on how to assess what is a "change", whether it deserves a safety assessment and what will be the extent of this safety assessment (See Chapter 2).

Chapter 2

What is a "change"?

The purpose of this chapter is to provide an approach for assessing whether a change in the ANS system needs a safety assessment or not.

There can be many reasons to make changes to an existing system, for example:

- to correct defects;
- to replace or update ageing equipment;
- to increase functionality;
- to modify procedures e.g. where there are efficiencies to be gained;
- staff changes

The provision of an air navigation service is inherently risky operation providing the primary means of avoiding aircraft collisions. Modern safety management practice rightly demands that before making a change, however small, to a safety related system we take appropriate steps to ensure that the change does not introduce an unacceptable risk into the system.

However, it is recognized there are many 'changes' made to the system on a day-to-day basis for which a formalised and recorded risk assessment is not undertaken, primarily because assessing each and every change would be an impossible task to achieve, while maintaining continuous provision of services. The aim of this chapter is to provide guidance in how to identify those "changes" for which a formal Safety Assessment is not necessary. In many cases such changes are already covered by an existing risk assessment – they are merely configuration changes within a safe 'design envelope'. The tactical implementation of such changes often involves an undocumented risk assessment undertaken by the person responsible for implementing the change.

There are very few circumstances under which the implementation of a change can be justified without a prior risk assessment. However, it is clear that if a hazard Identification process is undertaken and no significant risks are identified, then there is no safety benefit to be gained from further safety management activity. It is proposed therefore that a simple hazard identification (or hazard elimination) procedure might be appropriate to determine whether it is necessary to apply SAM.

Certain special circumstances may also provide justification for implementation of a change without a full implementation of SAM:

- If a system or a piece of equipment is known to be unreliable and/or unrepairable and the impact of failure is known and can be mitigated (such as might be the case with an obsolete piece of equipment) then it is probable that replacement with a more reliable alternative will provide a safety benefit. Even if the replacement were to fail it would be no worse than the previous situation. Under such circumstances it may be justifiable to implement the change before a full SAM assessment is possible. However it would be necessary to undertake such an assessment before such a change could be accepted as permanent. Note that in this situation, where the replacement system offers improved functionality it will often be the case that operational practices will be altered to take advantage of the improved functionality, thus failure of the replacement system may become more significant than failure of the system being replaced. Under these circumstances an assessment should be made of the change in working practices, either when assessing the introduction of the replacement system, or when implementing the new procedures.
- Under certain unpredictable circumstances (e.g. in an emergency) it can be necessary to operate a system in a non-normal manner in order to mitigate immediate risks. Under these circumstances it is normal to assess the situation rapidly as a tactical change and determine the optimum course of action. This process will involve a preliminary form of risk assessment, but not the detailed process described in SAM. However, due to the nature of the situation it may be necessary to implement the change anyway (see 2.3.3) .

It is important to note that the application of this guidance will be strongly linked to and reliant upon the ANSP safety management system (SMS), particularly for the following:

- Existing risk assessments and procedures – for reference and to generate new risk assessments;
- Safety Management and Quality Assurance system – procedures, document and records control;
- Competence management system – to ensure the competence of the ATM operations and maintenance staff;

- Change management system – to ensure all change proposals are formally assessed and approved/rejected and that suitable records are maintained;
- Project management procedures – to control the change;
- Safety occurrence reporting system – to ensure that urgent unplanned changes are followed up with the necessary risk assessments, etc. when time permits;
- Contingency planning and procedures – to ensure that all credible contingency requirements are addressed;
- The review process – to identify any necessary changes to the safety management system which are required;
- The argument developed to demonstrate that existing operations (so-called "legacy") are acceptably safe.

2.1 Changes subject to formal safety assessments

Major changes that directly affect safety and are not covered by previous Risk Assessments are immediately subject to a formal safety assessment. Proposed list which can be expanded and should be validated, approved and included in the ANSP Safety Management Manual:

- New system (people, procedure, equipment)
- New service
- Strategic change (see §2.3.1)
- Inclusion of a new waypoint
- Suppression of an existing waypoint
- Return to service of a previously suppressed waypoint
- Decommissioning of operational equipment that is no longer in use
- Changes to ink or paper in flight strip operational printers would be subject to an assessment (this involves testing but not Risk Assessment)

2.2 Changes not subject to formal safety assessments

The essential factors to be considered in determining whether a change is "subject to further assessment or not" should include the following as a minimum:

1. The number of sites to be affected by the change (nationally or by organisation).
2. The number of adjacent centres to be affected by the change (including across national boundaries).
3. The impact upon the ATCO's duties, including training, procedures, co-ordination role, equipment, Human-Machine-Interface, etc.

4. Similarly, the impact upon the pilot's duties.
5. The environmental impact, including the density of obstacles, mix of traffic, level of separation, airspace class, continuity of operations, etc.
6. The overall complexity of the change in its entirety (ensure that a change subject to assessment is not being achieved by means of a series of such changes not subject to assessment – "salami tactics").
7. The impact on technical publications including the need for derogation.
8. The project management aspects of the change, including leadership, timescales, resources, critical path, changing contingency, control of contractors, testing and commissioning, acceptance, etc. (This also has strong links with item 6.)

Note: Factors 6 & 8 have to be understood such that even if the change has no impact on the other factors (more operations related), the change could deserve an assessment due to factor 6 or 8 characteristics.

In addition to these criteria, a list (not exhaustive) of such changes is proposed here after:

- Instance of a Corrective maintenance (at the time of the action itself when maintenance staff perform corrective maintenance intervention, assuming that the "generic" procedure has to be assessed/accepted before being applied)
- Emergency operations (unknown till now, example: "9/11", "cas de force majeure")
- Material for administration offices (not on operational/simulation network)
- Connectors (as long as they are tested & tried)
- Some test equipment (for those which do not impact operational equipment and which do not require calibration)
- Training session (operational training: ESARR5-related + competency in ESARR3-related) (at the time of delivering a session of the training, but it assumes that the training plan and material have been assessed & accepted)
- Instance of Sector frequency change (assuming that the "generic" risk assessment was done prior)
- Split/combine sectors (no new sectors and assuming that the "generic" risk assessment was done prior)
- Actions on administrative rooms (cleaning, etc., excluding noisy, dusty or vibration-maker works)
- Specific weather conditions (not part of Ops manual, under time constraint)

- Decommissioning of administrative (non-operational) equipment
- Visitors (a simple but formal assessment should be done beforehand)

2.3 Strategic Change and Tactical Change

It is clear that changes applied to the ATM System can be classified as either strategic or tactical:

Strategic changes are those that are anticipated and planned and as such, a thorough risk assessment (in accordance with SAM) can be undertaken in advance of implementation. Typically this will include engineered changes to the system, such as new equipment or procedures or airspace, routes, SIDs and STARs or resectorisation (additional sector or change of the existing sectorisation) or LoA (Letter of Agreement).

Tactical changes are those that are necessary as a result of circumstances and situations that arise during operation of the system. These can include routine changes, such as opening and closing sectors or changing runway direction, or exceptional changes, such as use of a standby frequency or diversion of traffic due to bad weather. By their nature some unanticipated tactical changes may be implemented without the opportunity for an ad-hoc, formal and documented risk assessment in accordance with SAM (see §2.3.3).

2.3.1 Strategic Change

Strategic change is what might be considered the normal process of change in ATM. A strategic change will involve changes to one or more parts of the ATM system (people, procedures & equipment) which are applied with prior consideration and planning. Strategic changes would include, amongst others, changes to hardware or software in the ATM system, airspace redesign or changes to operational procedures or staffing arrangements.

When implementing strategic change SAM dictates that a formal risk assessment should be undertaken. Only if this assessment identifies that there are no risks associated with the change can the risk management activities be curtailed.

2.3.2 Anticipated Tactical Change

An anticipated tactical change may be defined as "*an urgent change to the operational system that has previously been planned for and associated risks have been assessed.*"

Some examples of anticipated tactical change are implemented after performing a safety assessment in accordance with SAM.

Many examples of anticipated tactical change will be considered to be part of normal operations, such as routinely combining sectors during quiet periods or change of active runway. Others may include exceptional, but predictable change, such as like-for-like replacement of parts under corrective maintenance, or emergency procedures (e.g. use of standby frequency) which should have been considered in any existing safety justification and associated risk assessment for the system under consideration.

Such anticipated tactical changes may be part of the "legacy design envelope": part of the system/service definition, but no safety demonstration was made, therefore they are considered as tolerably or acceptably safe using legacy argument. However, it is recommended that the ANSPs should survey such practices, identify the anticipated tactical changes which are operationally performed without any demonstration of their acceptable contribution to safety and gradually complete the missing safety assessment (e.g. perform "generic" safety assessment for like-for-like replacement).

Some of those exceptional tactical changes can be gradually anticipated by some ANSPs by learning from other ANSP occurrences (e.g. a 9/11 kind of scenario can now be defined and assessed by any ANSP).

When implementing anticipated tactical change (part of the "legacy design envelope" using legacy argument) it may be necessary to undertake a "tactical risk assessment", e.g. to determine the optimum time/conditions for implementing a runway change. There should be a recognised procedure (preferably a formal one) for implementing such anticipated tactical change and a person responsible for making such decision. However it is recognised that it is unlikely that this "tactical risk assessment" be documented, or be performed in accordance with SAM.

2.3.3 Unanticipated Tactical Change

An unanticipated tactical change may be defined as "*an urgent change to the established normal, degraded, or emergency Air Traffic Management operational regime which is not part of the emergency which in normal circumstances would have been addressed by means of a formal risk assessment, but the time (or other) constraints will only permit some subjective consideration of the risks and the best way to mitigate them.*" In this situation heavy reliance is placed upon the ATM staff's competence and experience, and almost by filling a subsequent incident report a review of the risk assessments would be required.

Its use therefore lies between where there is time to carry out a formal safety assessment for a change and where immediate action is required. Typically, this could range from a

few minutes to a few hours, and it is important to make the best use of this time to minimise risk.

In order to help defining "Urgent": its value should be expressed in number of minutes or hours.

A proposed checklist of aspects to consider with regards to an unanticipated tactical change is provided in Appendix A of this document.

2.4 Recommendations

It is recommended that the ANSPs include customized definitions (adapted to their environment) for each type of change described in this guidance material in their Safety Management Manual. In addition, criteria for each type of change as well as guidance on how to classify changes should be included in the SMS.

In particular three aspects need the endorsement of the ANSP Senior Management and the acceptance by the National Supervision Authority (NSA):

- List of changes not subject to further safety assessment;
- Criteria for classifying a change as "not subject to further safety assessment".
- Criteria for classifying a change as "urgent unanticipated change".

Chapter 3

Safety planning

Once a change has been assessed to be subject to a formal (full or shortened) Safety Assessment, the first step in initiating the SAM process is producing a formal Safety Plan. A Safety Plan describes the activities to be carried out throughout the SAM process project, detailing:

a) the scope of the project or system that is being considered (consider equipment, procedures and people aspects);
b) the safety activities planned to be carried in the different project phases
c) when or at what stage in the project the safety activities will be carried out;
d) the staff responsible for contributing to the safety activities; and
e) the accountable manager e.g. having the authority to approve safety documentation or having the authority to accept unresolved risks on behalf of the organisation etc.

The Safety Plan, in reality is a living document, and should be updated every step of the way, for each SAM phase and throughout the system life-cycle. To provide assurance of its suitability the plan must be approved by the Safety Committee and reviewed regularly. Not only can a Safety Plan be used to enable the project to be completed efficiently and without unexpected or unnecessary cost but it can also form a part of the argument in the Safety Case as assurance that safety has been adequately managed.

Early in the planning stage of a project, there may be some benefit in producing an outline of how it is intended to argue the safety of the system e.g. identifying the sort of safety assurance evidence that may be required. This outline can help to identify activities that need to be scheduled in the overall safety plan. What follows is an outline of the typical phases of a project that should be planned for. It should be noted, however, that each project is different and you may find that different, fewer or additional phases are more suited to a particular project.

3.1 Safety Planning Process

The default Safety Planning process is:

1. During the FHA, develop an Initial Safety Plan. It should describe the safety policy and justify the overall strategy adopted for the Project/Programme. It should also describe the **major activities** and **deliverables** identified for implementing the policy and strategy.
2. During PSSA, update the initial Safety Plan to define the safety assessment activities to be carried out during the System Design Phase. It should in particular describe the approach adopted to ensure that the system architecture is expected to achieve the specified Safety Objectives.
3. During SSA, update the Safety Plan to describe how the Safety Requirements are to be met. The Safety Plan should define the means for evaluating the fulfilment of Safety Requirements and the achievement of Safety Objectives. It should also specify specific procedures to be used during the operations and maintenance, and decommissioning of the System.

3.2 Responsibilities

Generally, the Project or Programme Manager should be responsible for the preparation of a Safety Plan and for ensuring that safety activities are carried out by properly trained, qualified and competent personnel.

The Project or Programme Manager may delegate the preparation of the Safety Plan to suitably qualified and competent personnel, but should retain the overall responsibility.

The Safety Plan should be formally reviewed by all persons, departments and organisations concerned by its implementation. Agreement should be gained on the contents and approved by the accountable manager.

Finally the Project/Programme Manager should ensure that all those involved in implementing the Safety Plan are informed of responsibilities assigned to them under the Plan.

3.3 Safety Plan Content

3.3.1 Size and depth

The size and depth of the Safety Plan will depend on the complexity and the safety criticality (risk level).

For simple Project or Programme, and systems presenting low risk, a simple Safety Plan defining the Project/Programme personnel and justifying the overall approach may be

sufficient. The Safety Plan may be included in a section of the overall Project/Programme Plan.

For more complex Project/Programme and systems presenting higher levels of risks, a complete Safety Plan should be developed. Several documents may be developed, for example, one document for the overall system and one document for each major sub-system.

More frequent updates may be required to reflect changes in, for example, the concept, the programme or the project organisation.

At any given time, the Safety Plan should give a valid overview of how the safety assessment process is being applied.

3.3.2 Defining the Overall Approach to Safety Assessment

This section outlines the tasks involved in defining the overall approach to safety within a Project/Programme:

- Define the overall Safety Policy and Strategy for the Project/Programme.

  Note: *To define the overall Safety Policy and Strategy for the Project/Programme, one could refer to the EATMP Safety Policy and describe how each policy statement and principle will be implemented in the Project/Programme.*
- Describe and justify the approach adopted for the safety assessment of the system.
- Describe the relationships between the safety assessment process and the system life cycle.
- Identify major safety deliverables and describe their relationships with the major milestones of the Project/Programme.
- Identify interfaces with other Projects/Programmes, if appropriate.
- Describe major assumptions on the system and/or its interfaces, that may have an impact on the safety of the system.
- Identify particular issues or features that may have an impact on the safety of the system (e.g., introduction of new technology).
- Identify persons, departments and organisations involved in the Safety Assessment process.

  Note. *Individuals include, for example, the Project/Programme manager, system and safety experts. Internal departments concerned include the safety department and safety review panels. Organisations include suppliers, contractors and*

consultants, end user representatives and regulators. Interactions between these organisations, and responsibilities for development, review, authorisation, approval and acceptance of the Project/Programme safety deliverables will be defined.

3.3.3 Structure of the safety plan

The Plan should document the outcomes of all the safety planning activities. It should be concise and readily comprehensible, and should refer to, rather than repeat material which is adequately documented elsewhere. For example, it is only necessary to document *differences* from the generic FHA process.

The Plan should be an aid to the project team, not an additional burden. It should be distributed to, or at least accessible by, all the organisations, departments and individuals involved. It is therefore important that it should be written in a way intelligible to readers with a wide range of experience and involvement with the system.

A possible structure for a Safety Plan is shown in Table 1.

Version control information

Date of latest revision, approval status.

Introduction

- Aims and objectives of the Plan.
- A high-level description of the Programme/Project objectives.
- A high-level description of the system purpose, operational scenarios, functions, boundaries, interfaces and operational environment.
- Scope of the Plan – Phases of safety assessment process covered by the current issue of the Safety Plan.
- Structure of the Plan.

Safety Criteria

- The regulatory and organisational requirements, and standards to be met, justifying their selection or the choice of an alternative approach where necessary.
- A justified statement of the specific targets to be applied to the system (e.g., any quantified Safety Objectives used in the Risk Classification Scheme), or of the approach to setting such targets.

Safety Assessment Approach

- Definition of the safety policy and strategy adopted by the Project/Programme.

Roles and Responsibilities

- Responsibilities for safety assessment activities – by organisation, department, job title on the Project and individual name.

Inputs, Activities, Methods and Outputs

- General description of the safety assessment activities to be performed, their inputs and outputs, the methods to be used

Safety Assurance Activities

- General approach for the Safety Assurance activities.

Schedule and Resource Allocation

Plans for the next stage

- Outline of how the next stages of safety assessment are expected to progress.

Table 1 - A Typical Structure for a Safety Plan

Chapter 4

The SAM Process

The SAM Process consists of three main phases:

- Functional Hazard Assessment (FHA);
- Preliminary System Safety Assessment (PSSA);
- System Safety Assessment (SSA).

These three phases are undertaken roughly following the timeline shown in Figure 4. The core activities of each phase are conducted at specific stages of the "change" process, and usually after the completion of the main activities of the preceding phase. However, due to the iterative nature of the entire process, supporting activities of each phase are conducted throughout the entire "change" as well as the system life-cycle.

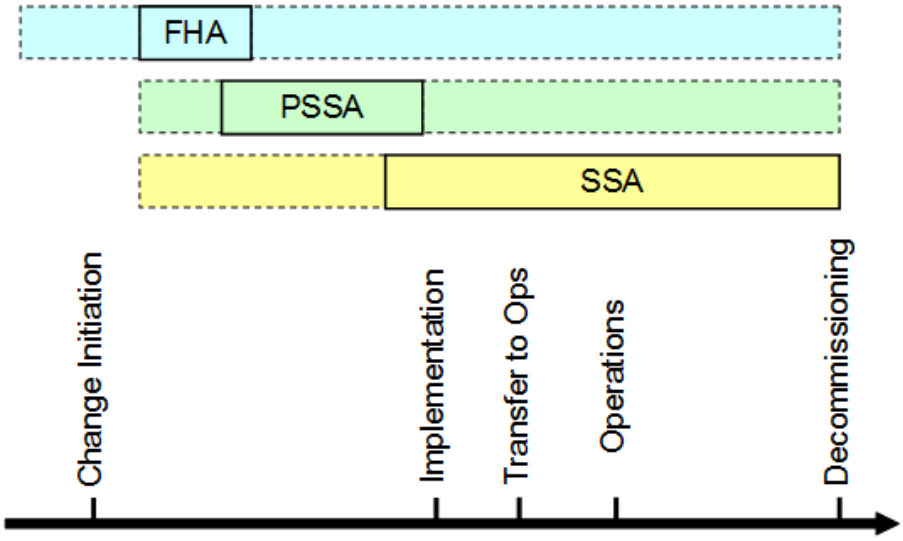

Figure 4 - SAM Timeline

This chapter serves as a brief introduction to the FHA, PSSA and SSA phases. Readers are however referred to additional guidance material on how to perform the activities of each phase, in order to support the correct and efficient implementation of SAM.

4.1 Functional Hazard Assessment (FHA)

Functional Hazard Assessment (FHA) is a top-down iterative process, initiated at the beginning of the development or modification of an Air Navigation System.

The objective of the FHA process is to determine: how safe does the system need to be.

The process identifies potential failures modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment.

The FHA process specifies overall ***Safety Objectives*** of the system, i.e. specifies the safety level to be achieved by the system.

4.1.1 When and how FHA is applied

The essential pre-requisite for conducting an FHA is a description of the high level functions of the system – such as would typically be specified in an operational concept document.

FHA is therefore first conducted during the ***System Definition*** phase of the system life cycle.

The purposes of the System Definition phase are to establish basic operational objectives for the system within its specified operational environment, to identify the functions required to achieve these objectives, and to specify system and interfaces (between functions and with the environment) requirements.

FHA is performed before the functions have been allocated to equipment, procedures or people elements: it considers what the proposed system will do, rather than how these elements should implement the functions. Indeed, FHA results will be used to support the process of function allocation.

In practice, however, development and assessment usually proceed in parallel, and some allocation of functions may already have been determined by practical constraints – especially where an existing system is being modified.

FHA can be applied at different levels. Ideally, FHA should be done at the overall Air Navigation Service or System level so that Safety Objectives are specified at the ANS level. On the other hand, Safety Requirements preferably should be derived on sub-

system elements during PSSA of this overall Air Navigation Service or System. In other words, in this ideal scenario there should be no need for FHA at sub-system level.

However, in practice, FHA is generally done at sub-system level and not at ANS level. Consequently, this methodology provides Guidance Material which addresses both ways of applying it.

FHA is an iterative process, therefore, it should be reviewed, revised and refined to cover lower level functions as the allocation of function is decided and the system design evolves.

4.1.2 FHA Overall Process

The FHA process is structured as a sequence of several steps. There are three key steps that have to be conducted whatever the size, complexity or organisational structure of the Programme/Project:

- **FHA Initiation**
  A level of understanding of the system, its operational environment and, if appropriate, its regulatory framework is developed.
- **Specification of Safety Objectives**
  During this step several important activities are conducted such as identifying potential hazards as well as the severity of their effects, and safety objectives are specified.
- **FHA Completion**
  During this step, all results of the FHA process are recorded and disseminated to interested parties.

The remaining two steps should be tailored to the size, complexity and organisational structure of the Programme/Project:

- **FHA Planning step**
  The objectives and scope of the FHA are defined as well as the activities to be carried out, their deliverables, their schedule and the required resources.
- **FHA Evaluation step**
  Safety Objectives and safety-related assumptions are verified and validated and assurance that activities have been carried out according to plan is provided.

During the FHA the most important activities are those concerning hazard identification and determination of the severity of the effects, which are illustrated in Figure 4. The activities conducted during the FHA phase should ultimately lead to a set of overall Safety Objectives which in turn determine how safe the system needs to be.

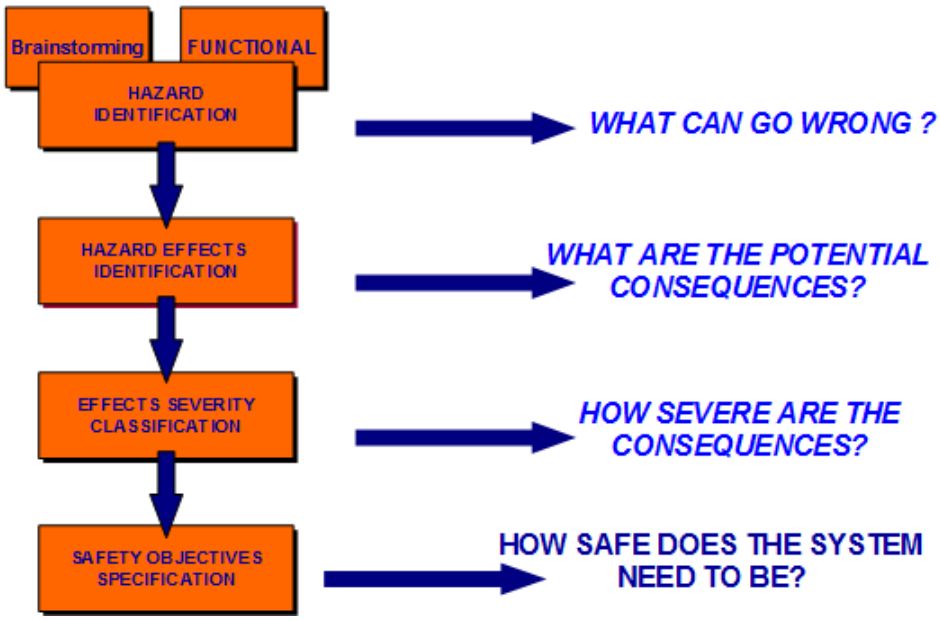

Figure 5 - FHA Core Activities

For detailed guidance material regarding the activities conducted in the FHA phase, readers are referred to TP-13 "SAM – Functional Hazard Assessment".

4.2 Preliminary System Safety Assessment (PSSA)

The ***Preliminary System Safety Assessment*** (PSSA) is the second of the three major steps in the generic process for the safety assessment of Air Navigation Systems. The PSSA seeks to answer the question "How Safe is the System Architecture?"

Preliminary System Safety Assessment (PSSA) is a mainly top-down iterative process, initiated at the beginning of a new design or modification to an existing design of an Air Navigation System.

The objective of performing a PSSA is to demonstrate whether the assessed system architecture can reasonably be expected to achieve the Safety Objectives specified in the FHA.

A **Safety Objective** [ESARR4] is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur.

A **Safety Requirement** [ESARR4] is a risk mitigation means, defined from the risk mitigation strategy that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.

The PSSA process apportions **Safety Objectives** into **Safety Requirements** allocated to the system elements, i.e. specifies the risk level to be achieved by the system elements. PSSA also identifies an Assurance Level per system element. This is also illustrated in Figure 5.

The system architecture can only achieve the Safety Objectives established during the FHA, provided the architecture elements meet their Safety Requirements.

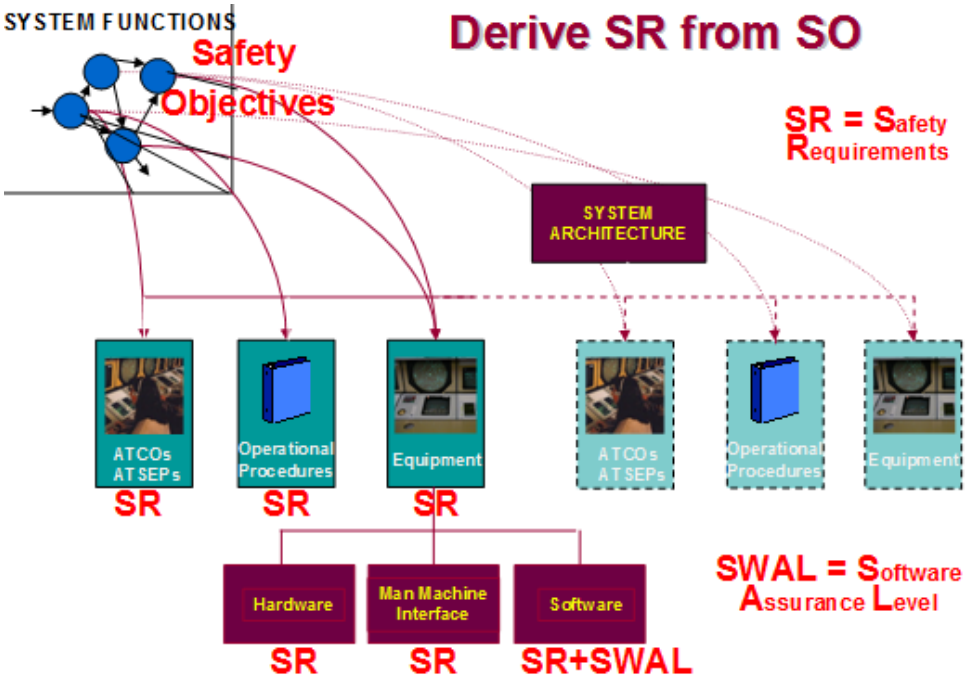

Figure 6 - PSSA - Deriving Safety Requirements for system elements

4.2.1 When and how PSSA is applied

PSSA is conducted during the ***System Design*** phase of the system life cycle.

A PSSA should be performed for a new system or each time there is a change to the design of an existing system. In the second case, the purpose of PSSA is to identify the

impact of such a change on the architecture and to ensure the ability of the new architecture to meet either the same or new Safety Objectives.

The essential pre-requisite for conducting a PSSA is a description of the high level functions of the system, with a list of assumptions, hazards and their associated safety objectives. All these are outputs of the FHA (Functional Hazard Assessment). The list of hazards and Safety Objectives comes primarily from FHA and is further completed during PSSA.

The Safety Assessment Methodology aims at limiting the number of iterations between system development activities and safety assessment. Development and safety assessment usually proceed in parallel.

PSSA is therefore an iterative process, which should be reviewed, revised and refined as the derivation of safety requirements and the system design (for non-safety reasons e.g. performance, interoperability, security,..) evolve. It provides guidance on how to identify the extent of the re-analysis required. It may even show that meeting Safety Objectives as identified by FHA cannot be achieved and consequently lead to a re-iteration of the FHA.

4.2.2 PSSA Overall Process

There are three key steps that have to be conducted whatever the size, complexity or organisational structure of the Programme/Project:

- **PSSA Initiation**
  Develop a level of understanding of the system design framework, its operational environment and, if appropriate, its regulatory framework.
- **Specification of Safety Requirements**
  Derive Safety Requirements for each individual system element (People, Procedure and Equipment)
- **PSSA Completion**
  To document and formally place the results of the whole PSSA process under a configuration management scheme and disseminate these results to all interested parties.

The remaining two steps should be tailored to the size, complexity and organisational structure of the Programme/Project:

- **PSSA Planning**

Define the objectives and scope of the PSSA, the activities to be carried out, their deliverables, their schedule and the required resources.

- **PSSA Evaluation**
  Ensure that Safety Requirements meet the Safety Objectives and that they as well as safety-related assumptions are correct and complete. Provide assurance that all PSSA activities are carried out according to plan.

For detailed guidance material regarding the activities conducted in the PSSA phase, readers are referred to TP-14 "SAM – Preliminary System Safety Assessment".

4.3 System Safety Assessment (SSA)

The ***System Safety Assessment*** (SSA) is the third of the three major steps in the generic process for the safety assessment of Air Navigation Systems. The SSA seeks to answer the question "Does the System as implemented achieve an acceptable risk?"

System Safety Assessment (SSA) is a process initiated at the beginning of the implementation of an Air Navigation System.

The objective of performing a SSA is to demonstrate that the system as implemented achieves an acceptable (or at least a tolerable) risk and consequently satisfies its Safety Objectives specified in the FHA and the system elements meet their Safety Requirements specified in the PSSA.

The SSA process **collects evidences** and **provides assurance** from implementation till decommissioning that the system achieves an acceptable (or at least a tolerable) risk and consequently satisfies its Safety Objectives and that the system elements meet their Safety Requirements and their Assurance Level.

SSA monitors the safety performances of the system during its operational lifetime.

For detailed guidance material regarding the activities conducted in the SSA phase, readers are referred to TP-15 "SAM –System Safety Assessment".

4.4 Configuration Management, Documentation and Records

A configuration management system should track the outputs of the different phases of the SAM process and the relationship between them.

Not only is it important that the SAM process is carried out correctly and completely, it is also important that SAM process should be clear and auditable.

The three important reasons are:

1. To demonstrate to third parties (including the regulator) that risks have been reduced to an acceptable level
2. To maintain a record of why decisions were taken, to ensure that further change does not invalidate the assessment or does not lead to unnecessarily repeating it;
3. To support the hand-over of safety responsibilities from one individual or organisation to another.

An appropriate and useable control scheme that ensures the origin, version control, traceability and approval of all documentation is recommended.

The extent of safety records maintained by a project will depend on the complexity and levels of risk involved. Safety records are difficult to replace so there must be appropriate security and backup to ensure that records are preserved. Up-to-date records should be kept throughout the system lifetime (including decommissioning).

A number of people will contribute to and need access to safety documentation, typically project staff, engineering staff, operational staff, safety specialists, managers and regulators.

The configuration management and documentation control schemes should include procedures to:

- To develop a configuration management plan;
- To establish a consistent and complete set of baseline documents;
- To ensure there is a reliable method of version identification and control;
- To establish and monitor the change management process;
- To archive, retrieve and release documents.

Appendix A

Unexpected tactical change checklist

The following checklist is intended to act as an "aide memoire" to help identify the key considerations, which should be addressed when considering an unanticipated tactical change.

1. Sources of assistance, information, advice and guidance		**Y/N (Ref)**
National Supervisory Authority guidance.		
Relevant procedure(s).	Identifying relevant information (e.g. limits) when procedures do not wholly apply.	
On-call/standby staff	If further staff are needed, or for advice.	
Senior management.	Should be consulted as a priority.	
Safety case/risk assessment.	The situation may have been identified but not fully addressed in terms of follow-up actions (e.g. procedures).	
Industry guidance.	Eurocontrol, ICAO, etc.	
Other ATM staff.	Locally and at other ATM centres.	
The regulator.		
2. Developing the change strategy		
Use all sources of information, advice and guidance.	Contingency plan	
Identify objectives that the change must satisfy.		
Consider any operational limitations that may have to be imposed.	To provide adequate mitigation of the risks. Full co-ordination with operations staff is required.	
Consider any changes to contingency planning.		
Use competent ATM staff to peer review &	Local or remote as necessary.	

validate the change.		
Gain approval from the highest authority immediately available.		
3. Communicating the change		
Identify all of those who need to be aware of the change.	e.g. other ATM centres, aircraft in and approaching controlled sectors.	
Inform the other stakeholders about the consequences of the change to their operational regime (not only notify but also gain some assurance of the correct understanding).		
Report the change as a technical incident.	Using the occurrence reporting system. This will ensure that the change is followed up with the necessary risk assessment and properly validated, etc.	
4. Records		
Take notes of key points in the decision-making process, information sources used, conversations with individuals contacted as log entries, etc.	As justification for the decisions made and their technical bases.	
5. Monitor		
Continue to monitor the change to ensure that it meets its defined objectives and that safety is not compromised.		
6. Ensure Continuity of Operations		
Prepare a brief for staff on the next shift to ensure they fully understand the implications of the change and the operating regime to be applied.		
7. Consider reverting to normal operations		
When a normal operating regime can be adopted consider how to safely revert to normal operations.	If necessary, repeat this checklist process as a change back to the normal regime.	