

EUROCONTROL



EUROCONTROL Guidance for Design of Contingency Strategies

(based on 'Current Practices' and Common Failure Modes Considerations)

*in support of
EUROCONTROL Guidelines for Contingency Planning
of Air Navigation Services*

Edition 1.0



DOCUMENT CHARACTERISTICS

TITLE

Guidance for Design of Contingency Strategies

(based on 'Current Practices' and Common Failure Modes Considerations) in support of EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services

PUBLICATIONS REFERENCE

- **ISBN Number:** 978-2-87497-012-2
- **ALDA Reference:**
EUROCONTROL-GUID-0109

DOCUMENT IDENTIFIER

- **Edition Number:** 1.0
- **Edition Date:** 15 February 2008

ABSTRACT

The aim of this document is to provide a high-level framework for ANSPs as they develop medium-term, Service Continuity plans to mitigate a broad range of security threats and safety hazards that might lead to the loss of a major facility. This framework is based on an assessment of current practices in designing strategies of alternative contingency strategies. The different approaches are not mutually exclusive and it may be necessary to use several different approaches. In addition, common failure modes as "pandemics" or "software bugs" are also discussed.

KEYWORDS

- Common failure modes
- Contingency
- Service
- Continuity
- Pandemics
- ANSP
- Strategies
- State
- Software bugs
- Aiding
- Failing

AUTHORS

Gerald Amar
Chris Johnson
Richard Lawrence

CONTACT(S) PERSON

Gerald Amar, DAP/SSH
Tel: +32 (0)2 729 36 93
Richard Lawrence, DAP/SSH
Tel: +32 (0)2 729 30 29

STATUS, AUDIENCE AND ACCESSIBILITY

STATUS

- Working Draft
- Draft
- Proposed Issue
- Released Issue

INTENDED FOR

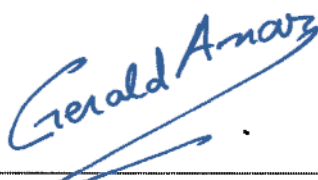

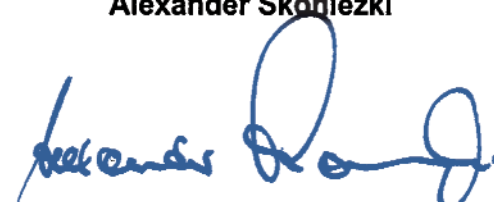
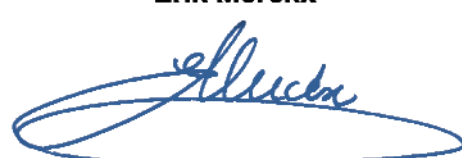

- General Public
- EATM Stakeholders
- Restricted Audience
- Electronic copies of this document can be downloaded from
http://www.eurocontrol.int/ses/public/standard_page/sk_sesis_guidelines.html

ACCESSIBLE VIA

- Intranet
- Extranet
- Internet www.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
Project Manager	Gerald Amar 	15.02.2008
Programme Manager	Antonio Licu 	18.02.2008
Head of DAP/SSH Business Division	Alexander Skonieczki 	18.2.2008
Deputy Director ATM Programmes	Erik Merckx 	25.2.2008
DAP Director	Guido Kerkhofs 	26.2.2008

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
Edition 1	15/02/2008	Released Issue	All

PUBLICATIONS

EUROCONTROL Headquarters

96 Rue de la Fusée

B-1130 BRUSSELS

Tel: +32 (0)2 729 4715

Fax: +32 (0)2 729 5149

E-mail: publications@eurocontrol.int

TABLE OF CONTENTS

DOCUMENT CHARACTERISTICS	1
DOCUMENT APPROVAL	2
DOCUMENT CHANGE RECORD	3
TABLE OF CONTENTS	4
TABLE OF FIGURES AND TABLES	5
EUROCONTROL GUIDELINES DISCLAIMER	6
ACKNOWLEDGEMENTS	7
FOREWORD	8
CHAPTER 1 - INTRODUCTION TO THE FIVE PHASE MODEL	9
1.1 Generic Contingency Life Cycle	9
1.2 From Theory to Current Practices	10
1.3 Inventory of Current Practice Strategies	12
CHAPTER 2 - DIFFERENT STRATEGIES FOR CONTINGENCY PLANNING	13
2.1 Generic Requirements Common to Contingency Strategies	13
2.2 Co-Located Facilities	15
2.3 Multi-Use Facilities (Training Development Units, Training Schools, Simulators)	18
2.4 Centralised (National) Facilities	21
2.5 ATS Delegation (International) - (Cross Border)	24
2.6 Shared Common Systems (International) - (Contingency Centres/Other Centres in Adjacent States)	27
2.7 Hybrid Models	30
CHAPTER 3 - SYSTEMS ENGINEERING PERSPECTIVE ON CONTINGENCY STRATEGIES	31
3.1 Different Engineering Approaches	31
3.2 'In-house' Engineering	31
3.3 Contractors and Sub-contractors	31
3.4 'Commercial Off the Shelf' (COTS) Approaches	32
3.5 Technical (International) Letters of Agreement	33
3.6 A Lifecycle Approach to Systems Engineering in Contingency.	33
3.3 Conclusion	34
CHAPTER 4 - VULNERABLE SCENARIOS AND COMMON MODE FAILURES	35
4.1 General	35
4.2 Common Mode Scenarios	35
4.3 Pandemics	35
4.4 Software Bugs	39
4.5 Internal Security Violations	39
4.6 Conclusion on Common Mode Failures	39
REFERENCES	40
GLOSSARY	41
Explanatory notes	41
Definitions	41
ABBREVIATIONS	44

TABLE OF FIGURES AND TABLES

FIGURES

FIGURE 1: GENERIC CONTINGENCY LIFE-CYCLE	9
FIGURE 2: KEY PHASES IN THE EXECUTION OF CONTINGENCY PLANS	10/11
FIGURE 3: GENERIC REQUIREMENTS OF THE KEY PHASES IN THE EXECUTION OF CONTINGENCY PLANS	14/15
FIGURE 4: CASE STUDY OF A SOLUTION USING CO-LOCATED FACILITIES FOR CONTINGENCY PLANNING	16
FIGURE 5: SWOT ANALYSIS OF CO-LOCATED FACILITIES FOR CONTINGENCY PLANNING	17
FIGURE 6: CASE STUDY OF A SOLUTION USING MULTI-USE FACILITIES FOR CONTINGENCY PLANNING	19
FIGURE 7: SWOT ANALYSIS OF A SOLUTION USING MULTI-USE FACILITIES FOR CONTINGENCY PLANNING	20
FIGURE 8: CASE STUDY OF A SOLUTION USING CENTRALISED (NATIONAL) FACILITIES FOR CONTINGENCY PLANNING	22
FIGURE 9: SWOT ANALYSIS OF CENTRALISED (NATIONAL) FACILITIES FOR CONTINGENCY PLANNING	23
FIGURE 10: CASE STUDY USING ATS DELEGATION (INTERNATIONAL/ CROSS BORDER) FOR CONTINGENCY PLANNING	25
FIGURE 11: SWOT ANALYSIS OF ATS DELEGATION (INTERNATIONAL/ CROSS BORDER) FOR CONTINGENCY PLANNING	26
FIGURE 12: CASE STUDY OF A SHARED COMMON SYSTEMS SOLUTION TO KEY STAGES OF CONTINGENCY PLANNING	28
FIGURE 13: SWOT ANALYSIS OF A SHARED COMMON SYSTEMS SOLUTION TO KEY STAGES OF CONTINGENCY PLANNING	29
FIGURE 14: SWOT ANALYSIS OF HYBRID MODELS FOR CONTINGENCY PLANNING	30
FIGURE 15: SUPPLIERS AND ANSP ENGINEERING STAFF VIS A VIS ATM LIFE CYCLE	33
FIGURE 16: CASE STUDY OF PLANNING FOR PANDEMICS (STRATEGY NEUTRAL)	38

TABLES

TABLE 1: WHO PANDEMIC PHASES	35
TABLE 2: ANSP CONSIDERATIONS DURING WHO PANDEMIC PHASES	36

EUROCONTROL GUIDELINES

DISCLAIMER

The guidance in this document is provided in support of the “EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services” that were made available to EUROCONTROL and ECAC Member States to provide guidance and support in advising their National Authorities and Air Navigation Service Providers (ANSP) in the development, promulgation and application of contingency plans in compliance with the Convention on International Civil Aviation, Annex 11, Chapter 2.30, on Contingency arrangements and Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services, Annex 1 § 8.2.

The “EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services” and subsequently this document are non-mandatory material, that is, general and procedural information developed by EUROCONTROL to support effective and harmonised development of contingency plans by the aforesaid States and/or their concerned ANSPs.

The information assembled in this document reflects the legislation in force on the date of publication of Regulation No 2096/2005 in the Official Journal of the European Union and of Amendment 45 to Annex 11 to the Convention on International Civil Aviation.

The compliance of the Member States, and their ANSPs, with their obligations under international law, the Single European Sky (SES) regulations and national legislation remains entirely their own responsibility. EUROCONTROL does not guarantee a particular outcome of an oversight exercise by the NSA on the compliance of the contingency plans developed by the States and/or their ANSPs nor does EUROCONTROL assume any liability for claims or damages sustained as a result of the implementation of these contingency plans.

ACKNOWLEDGEMENTS

The following Air Navigation Services Providers kindly agreed to participate in on-site visits to discuss their existing contingency measures that, subsequently, informed the development of this “Current Practices” document:

- Belgocontrol, Belgium
- MUAC, EUROCONTROL
- Nav Portugal, Portugal
- The LFV Group, Sweden
- NATS, UK

Special mention is made to Professor Chris Johnson, DPhil, University of Glasgow who was seconded to EUROCONTROL to conduct the on-site visits. Based on the information gathered during these visits and his own extensive knowledge of crisis/risk management issues, he compiled the core information and developed the ‘Current Practices’ elaborated in this document.

Finally, members of the EUROCONTROL Contingency Planning Task Force are thanked for their input, support and review of this document.

FOREWORD

In 2007, EUROCONTROL worked with a task force drawn from State Regulators and Air Navigation Service Providers (ANSPs) to draft guidelines for air navigation services contingency planning. The intention was to help Air Traffic Management (ATM) organisations prepare for the potential loss of a major unit (e.g. an area control centre) following possible scenarios that include, but are not limited to, terrorist actions, floods, fires and pandemics. As part of this work, a study was conducted to identify current and best practice in ATM contingency planning.

This document is part of a series of contingency planning guidelines released by EUROCONTROL. It is supplementary to, and should be read in conjunction with, the "EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services, Edition 1, October 2007 (hereafter "Guidelines") and its associated Reference Guide (RG).

Its aim is to present a number of potential contingency strategies, based around a common high-level framework, which can be used to help ANSPs' decision making process as they consider how to mitigate against a broad range of threats and hazards. The framework is based on the Five Phase Model included in the "Guidelines" and on an assessment of current practices in the design of contingency strategies.

A series of case studies are presented. These have been constructed following site visits to a number of ECAC ANSPs and reflect a variety of different strategies available to ANSPs to meet their contingency needs. Whilst some of the detail is based on theoretical plans of what ANSPs plan to do in the event of

contingency, much of it is based on actual contingency provision hence the inclusion in the title of "Current Practices". It is stressed that the strategies listed below are not mutually exclusive and it may be necessary to use several different approaches or combinations of approaches to meet ANSPs' needs.

These strategies include:

- Co-Located facilities.
- Multi-Use facilities.
- Centralised facilities.
- ATS Delegation .
- Common/shared system solutions.
- Hybrid models.

The intention is to provide a high-level overview of the managerial and organisational actions to prepare for and respond to a contingency; a variety of further perspectives should also be considered. These range from legal and regulatory provision through facilities management to security personnel. Each group contributes to the success or failure of contingency plans irrespective of whether a particular facility is co-located, centralised, multi-use etc. Brevity prevents a detailed analysis of the different strategies that might be adopted by each of these groups; the approach adopted by particular stakeholders will often be determined by local constraints. One critical element that should not be underestimated is the role of engineering and technical support in contingency. Differences in the approaches that are adopted by the organisations are explored.

The closing sections argue that some contingency scenarios require specialist plans. For example, pandemics often require that staffs are isolated to prevent

cross-contamination. This makes it difficult to develop 'Service Continuity' plans that involve the movement of ATCOs from a failing to an aiding unit. Other 'common mode' failures, such as software bugs are also described. These security threats and safety hazards jeopardize both primary and contingency facilities structured using any or all of the strategies mentioned in the earlier sections. The guidance concludes that these 'common mode' failures require particular attention from ANSPs during the development of contingency plans.

Every effort has been made to ensure consistency between the information in this document and the "Guidelines" and RG. Nevertheless, there are a number of differences since the information presented here is based largely upon operational reality rather than the more theoretical approach taken in the "Guidelines" and RG.

CHAPTER 1. INTRODUCTION TO THE FIVE PHASE MODEL

1.1 GENERIC CONTINGENCY LIFE CYCLE

The level of detail in the contingency plans prepared by ANSPs creates particular problems for the development of generic guidance material that might be used by ECAC States with a range of different operating profiles and resources. Consequently, the "EUROCONTROL Guidelines for the Contingency Planning of Air Navigation Services" (hereafter referred to as "Guidelines") and associated Reference Guide (RG) for Contingency Planning introduced the Generic Contingency Lifecycle model (see Figure 1) to provide a high-level model that can be used to guide the development of plans across all ECAC member States. ANSPs can map from these different stages of contingency to their own particular plans. The model does not assume any particular way of organizing ATM service, nor does it make any assumptions about the level of finance available for contingency provision.

The Life-Cycle should not, necessarily, be understood as a sequence of modes of operation. For instance, a Degraded Mode of Operation might be resolved before an emergency can develop and hence would lead directly to Recovery and Normal Operations. Similarly, in some situations, it might be necessary to move straight from 'Normal Operation' into 'Service Continuity'. The high-level model provides a structure or framework for the more detailed plans that each individual ANSP should develop to reflect their local context of operation.

The Life-Cycle is at a very high level of abstraction. For example, the following excerpt describes the process by which a contingency might be declared and recovery actions planned:

"The Centre Director is the only person who can decide if it is a crisis or not. The Supervisor calls the Ops Director they call the Centre Director and they then call the Director General. There is a concern to get the message out within the organisation before the 'press are at our gates'. Parts of this process are regularly tested 'at random'. There is a crisis room with telecoms but the crisis team NEVER gets involved in running the Ops room. The Director of Operations has responsibility for calling a contingency. The aim is to resume service provision within 48 hours. During this period appropriate software must be installed and dual or triple use hardware must be released for use in the contingency facility. In particular, it will be important during this period to:

1. Put in the voice communications systems necessary to move from a simulated scenario to operational service.
2. Convert from training, development and simulation to full operational systems.
3. Ensure power and other infrastructure provision including facilities management issues are addressed in another section of this report.
4. Deploy computer based training techniques and other competency systems to ensure that additional staff are 'up to speed' when the contingent facility goes live."

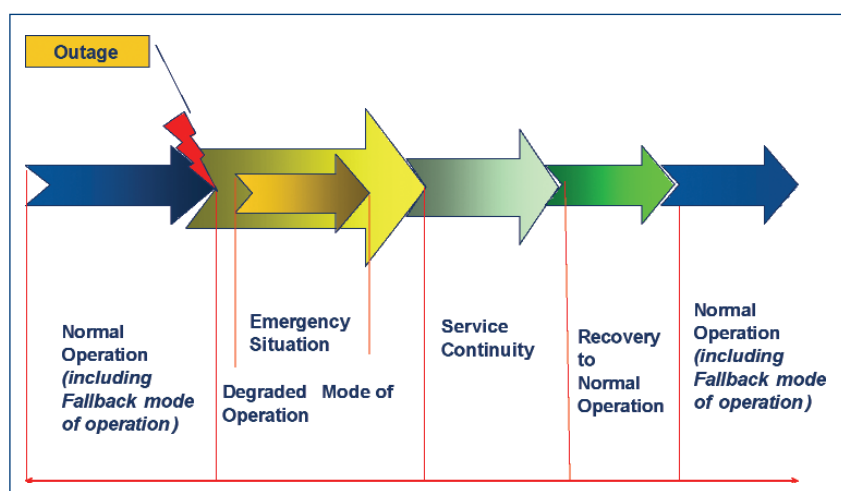


Figure 1: Generic Contingency Life-Cycle

1.2 FROM THEORY TO CURRENT PRACTICES

A lot of work is required to go from this basic template to the more detailed plans that should be prepared by individual ANSPs. In order to close this gap, a number of existing contingency plans were analysed and several site visits were organised with ECAC ANSPs. During these visits, it was possible to identify the level of detail that is required in particular contingency documents. One problem with developing 'case study' processes to this level of detail is that there are strong differences between ANSPs. The percentages of residual capacity are not the same nor are the assumptions about the types of resources that will be available. For instance, the previous citation assumes the presence of a dual-use facility close to the primary centre that is failing. The concern then becomes to migrate the contingency facility from its 'normal' role as a training and simulation centre to one in which it acts as a fallback facility. This approach

would not be useful for ANSPs that could not use their training and simulation facilities in this way. It was decided to try, therefore, to determine whether it was possible to identify a 'mid-way point' between the detailed arrangements that are particular to a single service provider, illustrated by the previous quotation, and the very high-level of abstraction in the Contingency Life-Cycle.

Figure 2 presents a comparison of the preparations that have been made by two ECAC States for contingency events. Based on different interpretations of the Five Phase Model described at Section 9.2 of the "Guidelines", the intention is to provide a more detailed sketch of the plans than those shown in Figure 1. This is done, however, without making the strong assumptions that are embedded within the textual contingency plans of particular States. Both of the ANSPs considered in Figure 2 have adopted an ATS Delegation approach (supported by international letters of agreement (LoAs)). In other words, if there is a failure in a

major centre then they have agreements to enable another centre, either within the same State or from a neighbouring State, to take over the operations of the failing unit.

The high-level sketches in Figure 2 and the Five Phase Model in the "Guidelines" can be further elaborated to provide a framework for 'case studies' in contingency planning. This level of detail is appropriate for the generic nature of the "Guidelines" because they allow for different instantiations by ANSPs as their plans change over time. In other words, it is relatively easy to see how these sketches might be changed, for instance, if letters of agreement were drawn up between three or more States rather than the international agreements that are shown in Figure 2. Finally, the models in Figure 2 also capture important differences in the strategy or approach that service providers have adopted to address adverse events.

ANSP INTERPRETATIONS OF FIVE-PHASE CONTINGENCY MODEL

ANSP A	ANSP B
<p>PHASE 0:</p> <ul style="list-style-type: none"> ● Transfer of aircraft in flight to the defined aiding unit. ● If feasible, take-over of the traffic on the frequencies of the aiding unit. ● Ensuring that all ATC units concerned are informed by the failing unit, or by the aiding unit, if required. ● Publication of prepared NOTAM. ● Inform CFMU. 	<p>PHASE 0:</p> <ul style="list-style-type: none"> ● A dangerous situation has been identified. ● The actual traffic situation should be secured. ● May be difficult to determine magnitude of problem and the duration of the outage. ● Must prepare fall-back instructions to ensure the safety of operations allowing a 'smooth' transition to phases 1-4. ● Appropriate authorities will identify the seriousness of the situation and initiate appropriate contingency measures.

ANSP INTERPRETATIONS OF FIVE-PHASE CONTINGENCY MODEL

ANSP A	ANSP B
<p>PHASE 1: IMMEDIATE MEASURES</p> <p>Short-term contingency measures and the delegation of air traffic services to an aiding unit. This phase only starts once all safety measures in phase 0 are in place.</p> <p>Will adopt either:</p> <ul style="list-style-type: none"> ● Conflict-free contingency route system. ● Delegation of ATS to aiding unit. ● Or mixed models. 	<p>PHASE 1: IMMEDIATE ACTIONS:</p> <p>Phase 1 mainly focuses on the safe handling of aircraft in the airspace of the failing unit, using all technical means still operationally available.</p> <ul style="list-style-type: none"> ● Evacuation of the airspace. ● Contingency measures should be initiated. ● Notification of all concerned. ● Determination and coordination of flow control measures. <p>Delegation of ATS will be initiated where appropriate.</p>
<p>PHASE 2: RELOCATION OF WORKING POSITIONS</p> <p>If control centre is inoperative for a longer period of time:</p> <ul style="list-style-type: none"> ● Working positions will be relocated and personnel will be transferred to aiding unit(s). ● Personnel management and local regulations will remain unchanged. ● Escalation phase II designates beginning of the staffing of relocated working position and the resumption of control services in a different environment via Letter of Agreement 	<p>PHASE 2: RELOCATION:</p> <p>Phase 2 starts when staffs of the failing unit arrive at the aiding unit(s).</p> <ul style="list-style-type: none"> ● Detachment of staff to the aiding unit(s). ● Opening of contingency working positions at aiding unit(s). ● Stabilization of new situation. ● Improving the flow capacity. ● ICAO route structure and sectorisation in failing unit should remain unchanged. ● All technical means should be made available to establish and maintain communication necessary to provide ATS in the failing unit.
<p>PHASE 3: OPTIMISATION</p> <p>If the relocation persists for a longer period of time, an optimisation of work flows and consequently an increase in capacity will take place in phase III.</p>	<p>PHASE 3: OPTIMIZATION AT AIDING UNIT(S).</p> <p>Staff of the failing unit should become familiar with the operational facilities of the aiding unit. The aim is to optimise capacity with the available resources within the published ICAO route and sectorisation structures. Means of communication should be upgraded as much as is possible. Coordination procedures should revert back to 'normal' handling.</p>
<p>RECOVERY PHASE:</p> <p>Operations manager initiates damage analysis after contingency has occurred. Measures to restore operations will then be taken. Once operations have been restored, the operations manager at the failing unit will inform the aiding unit and the failing unit will resume ATS after coordination with the others.</p>	<p>PHASE 4: RECOVERY ACTIONS:</p> <p>Revert back to the original unit and working position; Coordinate the start of normal operations. A Transition plan should be started taking into account technical and operational conditions. As soon as the failing unit has decided to revert back to the original facilities, the appropriate authority of that unit should inform all partners. The failing unit must co-ordinate the time at which normal operations can be resumed. Updates must be implemented to flight plan and radar data processing systems.</p>

Figure 2: Key Phases in the Execution of Contingency Plans

1.3 INVENTORY OF CURRENT PRACTICE STRATEGIES

The site visits to different ECAC States helped to identify important variations on the approaches described in Figure 2. Both ANSP A and ANSP B assume that it will be possible to relocate service provision under contingency using agreements with aiding units either inside the same country or with neighbouring ANSPs. In contrast, the site visits also identified a number of alternative strategies that are intended to support operations when a failing centre declares a contingency:

1. **Co-Located Facilities (National):** Other States have chosen to develop limited contingency facilities on the same sites as the primary centres. For example, training and test suites can be reassigned for contingency work. This reduces costs through dual use but has limitations. Some scenarios, including floods, fires, earthquakes and security threats could wipe out both primary and contingency resources. Military facilities may also be considered although these have not been mentioned by the States visited.
2. **Multi-Use Facilities (National) - (Training Development Units, Training Schools and Simulators):** In order to ease the costs of contingency provision, backup systems may be redeployed from training and simulation should a primary facility fail. This creates problems when contingency managers need to access the shared resource to run recuperation drills; the resource would then not be available for use

by other members of an ANSP. Conversely, during a contingency the training and simulation facilities that might otherwise be used to debug system failures would not be available to engineering teams because they would be needed as the primary contingency facility.

3. **Centralised Facilities (National):** Single contingency centres can be developed to cover several ATM units. This reduces the costs of international letters of agreement and redundant resources if contingency facilities are provided for each centre within a country. However, there are significant overheads in making sure that the single national contingency centre keeps pace with changes in all of the other regional sites.
4. **ATS Delegation (International) - (Cross Border):** This approach assumes that ANSPs will draft collaborative agreements with neighbouring States so that they will assume responsibility for some of their workload under contingencies. This can be flexible and cost effective. However, it requires both technical (e.g. frequency/surveillance cover) and political agreement. This can be difficult if there is any perception that control will be surrendered for some portion of national airspace even under a contingency. It can also be difficult to coordinate the drills that are required to ensure that these agreements are worth more than the paper they are written on. Licensing issues associated with provision of services in another State's airspace would also need to be confirmed.

5. **Shared Common System Solutions (International) - (Common Contingency Centres/Other Centres in Adjacent States):** Several States in a region can share a common but dedicated contingency facility. This has obvious benefits in terms of initial costs to set up and it avoids some of the problems associated with an aiding unit (e.g. another State's primary site) using their existing capacity for running the services of another ANSP. However, there are also considerable practical drawbacks from the development of regional contingency centres. There will be high continuous (variable) costs in order to ensure that the software and staff in the regional centre can be configured to meet the needs of three or more different States. Hence, it may be more realistic for ANSPs to agree amongst themselves combinations of pairs or groupings based around shared/common systems (e.g. FDPS procured from the same software and/or hardware manufacturer) although the data and sectorisation are likely to be different.
6. **Hybrid Models:** It is also possible to mix models, for example, accepting some of the costs of a regional solution but also retaining short term contingency facilities in a national centre or Training Academy. This may offer greater flexibility for both safety and business continuity.

CHAPTER 2. DIFFERENT STRATEGIES FOR CONTINGENCY PLANNING

By combining information gathered during site visits and the information in the Five Phase Model in the “Guidelines”, it has been possible to draw up a list of generic requirements that are common to the contingency strategies described in this document; these are presented in §2.1. The specifics for each strategy are then described in more detail in sections 2.2 to 2.6 including:

- The additional requirements needed to fulfil each element of the Contingency Framework.
- A SWOT analysis of each strategy is presented that brings together the Strengths, Weaknesses¹, Opportunities and Threats that can be associated with each strategy.

The aim is to present the potential contingency strategies to help ANSPs’ decision making processes as they consider how to develop ‘Service Continuity’ to mitigate a broad range of threats and hazards that might lead to the loss or prolonged disruption of a major ANS facility. It is stressed that the strategies are not mutually exclusive and it may be necessary to use several different approaches or combinations of approaches to meet ANSPs’ needs.

2.1 GENERIC REQUIREMENTS COMMON TO CONTINGENCY STRATEGIES

Brief details of the characteristics of the generic requirements that populate each stage/phase of the Contingency Framework are as follows:

In the Planning stage

Preparations of Plans, covers some of the basic ingredients needed to build a contingency plan - there is much more detail in the ‘Policy’, ‘Plan’ and ‘Achievement’ sections (and related Appendices) of the “Guidelines”.

Fail to Safe

This stage describes the Phase 1, Immediate Actions that, typically, might be expected to be taken by ANSPs during the very early (first 30 - 60 minutes) of a contingency situation to preserve the safety levels of aircraft in flight. This could involve measures such as ‘clear the skies’² techniques and internal and external notification. Phase 2, describes short to medium term actions that would normally be taken within the first 48 hours of an event triggering a contingency scenario. These measures would typically stabilise the situation in preparation for longer term arrangements that might be needed to facilitate ‘service continuity’ provision of air navigation services. Further detail on these activities can be found in the ‘Execution and Assurance’ section of the “Guidelines”.

Service Continuity

The Service Continuity stage considers those actions that will facilitate a move towards longer-term contingency

operations. Issues related to the relocation of staff are presented under Phase 3, whilst Phase 4 covers the optimisation of service provision in contingency conditions such that capacity can be increased gradually to the levels agreed previously with end-users and States authorities.

Recovery

The Longer term response and Recovery stage (Phase 5) briefly describe the essential issues related to the reversion/transition back to ‘Normal’ operations (see Life Cycle in §1.1). These include the likely requirement to conduct ‘shadow’ or ‘parallel’ operations in some circumstances as a precaution until the integrity of the ‘failed’ unit has been assured.

Maintenance

Maintenance of Plans, lists the essential maintenance activities (de-briefing, feedback, review, revision etc) that should be conducted as part of proactive change management to ensure that contingency measures remain up to date and viable - more extensive information is provided in the “Guidelines”.

Note: *This document focuses on designing strategies for ATM facilities. While designing contingency plans, supporting systems and services should also be considered. For instance, requirements for CNS external facilities/sites (eg. radars, radio stations) supporting control centre(s) to have appropriate contingency plans in place: minimum radar coverage may be required in contingency for radar system in case of the degradation of number of radar sources. Reference can also be made to the “Guidelines” Appendix G.*

¹ Weaknesses refer to circumstances that are already present and could affect a contingency strategy now, whereas ‘threats’ are circumstances that are not yet present but might affect a contingency strategy in the future.

² For the context of this document only, ‘clear the skies’ is understood as described in section 5.1 of this document.

GENERIC REQUIREMENTS

PLANNING

PREPARATION OF PLANS

- Establish requirements for contingency.
- Identify key resources including facilities management.
 - *Ensure key personnel in ANSPs (i.e. potential failing and aiding units) are provided with means to communicate at short notice.*
- Establish contingency planning group.
- Ensure early engagement with Regulator/NSA as necessary:
 - *e.g. obtain approval from regulators and State authority for procedures and practices that affect the airspace of the failing unit.*
 - *e.g. clarify licensing and training issues when staff may be providing safety related services for the airspace of a neighbouring country.*
- Ensure training of staff (ATCOs and ATSEP) in contingency measures.
- Document contingency plans.
- NSA(s) to verify the existence and content of contingency plans.
 - *In case of cross-border provisions of services in case of contingency, NSAs of both failing and aiding units should verify contingency plans.*

FAIL TO SAFE

Phase 1 - Immediate Actions

A dangerous situation has been identified. Focuses on the safe handling of aircraft in the airspace of the failing unit, using all technical means still operationally available.

- Secure actual traffic situation.
- Consider, evacuation of the airspace - 'clear the skies'.
- Try to determine the magnitude of problem and the duration of the outage.
- Prepare fall-back instructions to ensure the safety of operations allowing a 'smooth' transition to phases 2-5.
- Appropriate authorities will identify the seriousness of the situation and initiate appropriate contingency measures.
- Initiate process of informing all interested parties.

Phase 2: Short/Medium Term Actions (<48 hours)

Focuses on stabilising the situation and, if necessary, preparing for longer term contingency arrangements:

- Contingency measures should be initiated.
- Complete notification of all concerned.
- Determine and coordinate flow control measures.
- Initiate delegation of ATS, where appropriate.

SERVICE CONTINUITY

Phase 3: Relocation

Starts when staff of the failing unit arrives at the aiding unit(s):

- Detach staff to aiding unit(s).
- Open contingency working positions at aiding unit(s).
- Stabilise new situation.
- Staff of the failing unit should become familiar with the operational facilities of the aiding unit.
- Improve the flow capacity.
- Maintain the published or introduce a reduced ICAO route structure and sectorisation in the failing unit.
- Utilise all technical means to establish and maintain communication necessary to provide ATS in the failing unit.

Phase 4: Optimisation

The aim is to optimise capacity gradually up to maximum potential (within the published or reduced ICAO route and sectorisation structures in line with previously agreed end-user and regulator expectations.

- Upgrade means of communication as much as is possible.
- Use 'normal' coordination procedures as much as possible.
- Consider any knock-on consequences or 'domino effects' on third-party ANSPs/states who will be affected by the increase in workload for the aiding units.

GENERIC REQUIREMENTS

RECOVERY

Phase 5: Longer-term Response and Recovery

The aim is to revert back to the original unit and working position in a safe and orderly manner:

- Initiate Transition Plan - taking into account technical and operational conditions.
- Inform all interested parties of intention to revert to 'Normal' operations.
- Assign staff between failed unit and contingency facility for 'shadow' or parallel operations during transition period.
- Co-ordinate the time at which normal operations can be resumed.
- Implement updates to flight plan and radar data processing systems.
- Authorise the resumption of 'Normal' operations.

MAINTENANCE OF PLANS

- Hold immediate 'hot' debrief
- Conduct 'lessons learned' exercise after actual or practice demonstrations of contingency plans.
- Revise contingency planning arrangements and promulgate changes as necessary
- Ensure contingency planning is part of organisation's "Change management" processes.

Figure 3: Generic requirements of the Key Phases in the Execution of Contingency Plans

2.2 CO-LOCATED FACILITIES

There are similarities between the Co-Located and Multi-Use strategies. It is common place for ANSPs using co-location strategies to also exploit a Multi-Use approach so that they do not have large secondary control rooms that are sitting 'empty' or infrastructure components that are 'idle' during long periods of normal operation. However, not all dual use facilities are Co-Located. Some ANSPs propose the development of national centres on their Academy sites which are in some cases a short distance away from any of the major national control centres.

In other circumstances it may be possible, with prior agreement, to utilise military facilities that may be Co-Located within a civilian facility.

Reference can also be made to the "Guidelines"; Appendix C - Alternate Contingency Location Strategies.

GENERAL CHARACTERISTICS

- Contingency facilities can be developed on the same sites as the primary centres - e.g. training and test suites can be reassigned for contingency.
- Obsolete systems may be used as a fallback facility.
 - *These applications can be retained on a 'care & maintenance' basis that enables ops teams to use them if the primary system fails; they provide considerable additional assurance during operations to 'clear the skies'.*
 - *However, some old systems may only be used for 'clear the skies' operations and may not be approved for use during higher traffic loadings.*
 - *Additional training may be required for staff who will be servicing and using the obsolete(fall back) systems*
- As part of the Immediate and Short-Term Actions, it may be possible for staff to begin configuration of the contingency facility to take over from the primary system.
 - *Depending on the extent of this task, it may be possible for the contingent system to assist in 'clearing the skies'.*
- A Short to Medium-Term action would be to gain management support and approval to confirm the dedicated use of shared, Co-Located facilities for contingency operations.
- It is important during the Relocation phase that systems teams validate both the technical infrastructure and also the data that is used to configure contingency systems.
- Management and coordination may be undermined by large numbers of staff wanting to 'lend a hand' in the immediate aftermath of an incident.
 - *This can create problems because these staff may be needed later on as the initial watches come off shift.*
 - *There is also a danger that they will interfere and place additional demands on security and facilities management. Many groups should be sent home and should come in when explicitly required.*

³ Care and maintenance' refers to maintaining the operational capability of redundant obsolete system at an agreed level of operational readiness.

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of a solution using Co-located Facilities for Contingency Planning:

SPECIFIC REQUIREMENTS	
PLANNING	
PREPARATION OF PLANS	
<ul style="list-style-type: none"> Establish co-located facility. If necessary, establish agreements with dual use groups for training time and for access conditions under contingency. 	
FAIL TO SAFE	
Phase 1: Immediate Actions	
<ul style="list-style-type: none"> Inform other users of a co-located facility of a potential incident. Obtain management permission to requisition shared resources. Take initial steps to reconfigure the Co-located facility. Consider use of contingency facility for 'clearing the skies' if a 'hot swap' is possible. Consider potential incidents involving contingency facility. 	
Phase 2: Short/Medium -Term Action (<48 hrs)	
<ul style="list-style-type: none"> Complete configuration of co-located facilities. Initiate contingency for security/facilities management etc at Co-located site. Establish back-ups for other users of Co-located resource, especially systems teams and training for watches to back-up initial users of contingency facility. Plan for gradual hand-over to Co-located facility, depending on contingency. 	
SERVICE CONTINUITY	
Phase 3: Relocation:	
<ul style="list-style-type: none"> Relocation should be minor in terms of physical move to adjoining site. Sectorisation changes may be needed if the Co-located facilities have fewer positions/resources than primary site. Ensure systems team validate reliability of data and communications infrastructure not just as Co-located facility goes 'live' but also during initial operation. Secure lines of command and management by allowing only necessary staff to remain on-site. 	
Phase 4: Optimisation at Co-located Unit	
<ul style="list-style-type: none"> Bring in additional staff to ensure adequate rest and rotation of shifts/watches. Train additional staff on Co-located facility to aid shift rotation etc. 	
RECOVERY	
Phase 5: Longer-Term Response and Recovery	
<ul style="list-style-type: none"> Release shared resources. 	

Figure 4: Case Study of a Solution using Co-located Facilities for Contingency Planning

The Strengths, Weaknesses, Opportunities and Threats associated with a Co-Located strategy for contingency planning are shown below:

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● Relatively quick and easy to implement when such facility exists. ● Reduces costs through potential dual use of facilities; logistics and facilities management are eased. ● Use of redundant/obsolete systems provides considerable additional assurance during operations to 'clear the skies'. ● Minimal relocation issues during Relocation (Phase 3). 	<ul style="list-style-type: none"> ● Old systems might not be approved for use during higher traffic loadings or prolonged periods. ● Additional training may be required for staff who will be servicing and using the obsolete(fall back) systems. ● Competing requirements (contingency versus other usage (training, engineering etc)) may create problems. <ul style="list-style-type: none"> ● <i>Resource cannot be used for 2 purposes at the same time, might induce delay.</i> ● <i>Contingency systems may be needed to debug failure during contingency.</i> ● Changes in sectorisation will probably be required in most cases; there are unlikely to be as many positions in the contingency facility as there are in primary control rooms. ● The possible take over of military control equipment would be subject to prior agreement. ● Considerations must be given to ensure that military infrastructures can support civil operations with the same levels of safety. <ul style="list-style-type: none"> ● <i>'Certification' of military facilities should be considered.</i> ● Some scenarios would wipe out primary and contingency resources - see Chapter 4 Section 4.2 on 'Common Mode Scenarios'. ● Over time, the focus on the contingency role (of the infrastructure) may be downgraded.
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● Optimise the replacement of older systems: roll-back and re-use older systems for contingency purposes. ● May also help improve training/simulation facilities at same time. ● Civil/Military cooperation could be improved if military facilities are chosen for contingency operations. 	<ul style="list-style-type: none"> ● Could be difficult to sustain if seen to undermine the advance and facilitation of FAB and SESAR concepts and objectives.

Figure 5: SWOT Analysis of Co-Located Facilities for Contingency Planning

2.3 MULTI-USE FACILITIES (TRAINING DEVELOPMENT UNITS, TRAINING SCHOOLS, SIMULATORS)

There are similarities between the Multi-Use and Co-Located strategies. Some ANSPs using Multi-Use strategies also exploit a Co-Located solution. However, this is not always the case and some ANSPs propose the development of national centres based on their training/simulation facilities which are in some cases a short distance away from any of the major national control centres. Reference can also be made to the "Guidelines", Appendix C - ATS Training and Development Units.

GENERAL CHARACTERISTICS

- Dual-use of certain infrastructures (e.g. training and test suites, simulators etc) may or may not be re-assigned and developed on the same sites as the primary centres.
- The initial planning phases should carefully consider any resources that are shared with other groups inside an ANSP.
 - *It is critical that the other users of the shared systems can free the resource when it is required and that the resource can be brought on-line for contingency purposes.*
 - *Many dual use contingency facilities are also used for training and simulation or for system development when they are not being used in an emergency.*
 - *This is particularly important for teams of co-workers who might need the resources to support recovery operations. Examples would include workstations that are used for contingency operations but which would otherwise support the training of staff or the systems teams who need to diagnose the causes of any failure.*
- As part of the Immediate and Short-Term Actions, it may be possible for staff to begin configuration of the contingency facility to take over from the primary system.
 - *Depending on the extent of this task, it may be possible for the contingent system to assist in 'clearing the skies'.*
- A Phase 2 Short to Medium-Term action would be to gain management support and approval to confirm the dedicated use of shared, Multi-Use facilities for contingency purposes.
- Phase 2 should also consider facilities management and site access/security as the contingency facility becomes active.
- It is important during Relocation (Phase 3) that systems teams validate both the technical infrastructure and also the data that is used to configure contingency systems.
- Management and coordination may be undermined by large numbers of staff wanting to 'lend a hand' in the immediate aftermath of an incident.
 - *It could create problems because these staff may be needed later on as the initial watches come off shift.*
 - *There is also a danger that they will interfere and place additional demands on security and facilities management.*
 - *Many groups should be sent home and should come in when explicitly required.*

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of a Solution using Multi-Use Facilities for Contingency Planning:

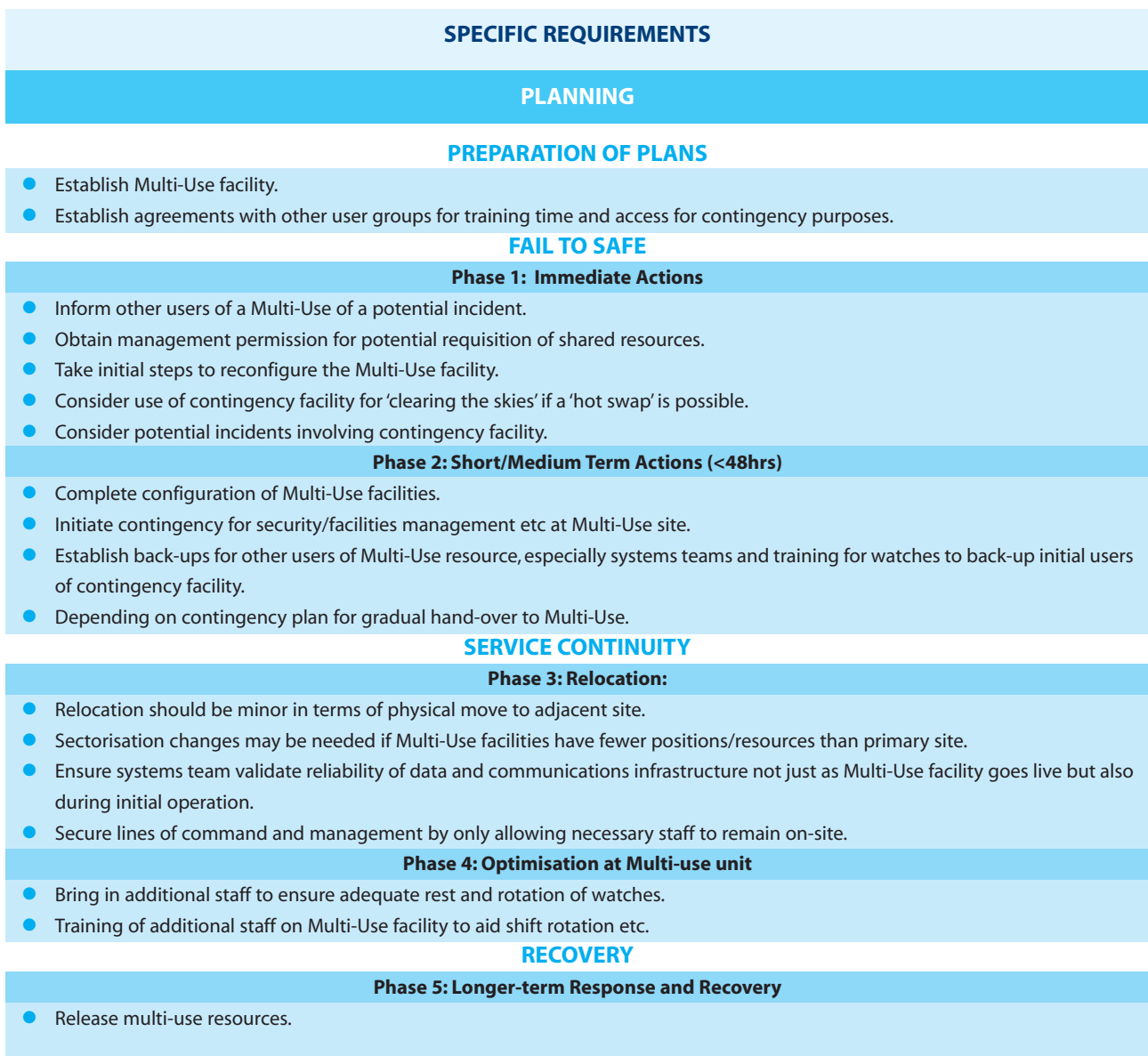


Figure 6: Case Study of a Solution using Multi-Use Facilities for Contingency Planning

The Strengths, Weaknesses, Opportunities and Threats associated with a Multi-Use of facilities strategy for contingency planning are shown below:

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● Reduces costs through potential Multi-Use of facilities. ● Multi use ensures that key elements of the contingency infrastructure are adequately maintained. ● Use of redundant/obsolete systems provides considerable additional assurance during operations to 'clear the skies'. ● If facility on or close to the primary failing site then there should be minimal Relocation issues. 	<ul style="list-style-type: none"> ● Multi-use facilities may not be approved for use during higher traffic loadings or prolonged periods. ● Competing requirements (contingency vs other usage (training, engineering etc)) creates problems. <ul style="list-style-type: none"> ● <i>Potential delays in switching to contingency configuration.</i> ● <i>Resource cannot be used for 2 purposes at the same time, might induce delay in re-configuration.</i> ● <i>Contingency systems may be needed to debug failure during contingency</i> ● Changes in sectorisation will probably be required in most cases; there are unlikely to be as many positions in the contingency facility as there are in primary control rooms. ● If the dual use facility is located away from the primary failing site then there may be associated relocation issues to consider. ● Some scenarios would wipe out primary and contingency resources - see Chapter 3 Section 3.2 on 'Common Mode Scenarios'. ● Over time the focus on the contingency role (of the infrastructure) may be downgraded.
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● May also help to improve training/simulation facilities at same time. 	<ul style="list-style-type: none"> ● Could be difficult to sustain if seen to undermine the advance and facilitation of FAB and SESAR concepts and objectives.

Figure 7: SWOT Analysis for Multi-Use facilities for Contingency.

2.4 CENTRALISED (NATIONAL) FACILITIES

The Centralised strategy described below relates to a single national centre as opposed to any international element which is covered in the Common Systems strategy. Many aspects of the Centralised strategy are similar to those described in the Co-Located and Multi-Use sections; however, they are not mutually exclusive. For instance, even in a Centralised system it is likely that for convenience the national centralised contingency centre will be Co-Located with at least one ATM centre. However, this is not always the case, for example, one ANSP has plans for a centralised contingency facility to be established within their training school which is Co-Located with their management facility and not close to any of the major operational centres. This is justified on economic grounds because the contingency facility could be used as a dual use simulation and training centre. *Reference can also be made to the "Guidelines", Appendix C - Alternate Contingency Location Strategies.*

GENERAL CHARACTERISTICS

- A single national contingency centre within each State which will provide cover for all ATM service operations in one place.
- As dictated by the contingency requirements decided at the Policy stage (see Guidelines), the Planning process begins by identifying an appropriate strategic location for the central contingency facility.
 - *This is not simply a technical decision; it will be determined by national infrastructures and geography.*

- *It is also political because employees in other sites may feel threatened by the centre's ability to replicate some portion of the outlying centre's 'normal' traffic flows. Social dialogue may be required to address this issue.*
- It is likely that the centralised facility will need to be supplemented by more localised support including mobile towers.
- If ANSP common systems can be utilised for Centralised facility then opportunities for economies of scale will exist.
- During the Immediate Actions phase, other users of the shared, centralised facility must be alerted that a failing unit may call upon this scarce resource.
- Some initial reconfiguration may take place in anticipation of a contingency being declared - this may depend upon the level of staffing available at the national contingency centre.
- During the Immediate Action phase it may be possible to conduct a 'Hot Swap' from the failing unit to the contingency facility before the 'skies are cleared' if the contingency facility is well supported and the configuration issues are relatively straightforward.
 - *However, this needs a greater degree of training and coordination which may be possible in a centralised facility within a single national system.*
- Decisions should be made about the best allocation of human resources between the failing and the centralised unit.
- Staff need to be rested; shifts rotated and training delivered to ensure that operations are optimized in the centralised contingency unit.
- In the case of centralised facility, feedback is particularly important:
 - *It is important to determine what impact the transition to a centralised national facility had upon the workload of the adjacent units as they adjust to hand-over from the failing centre.*
 - *Possible shortcomings may raise the political issues that often complicate the establishment of single, centralised facilities.*

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of a Solution using Centralised (national) facilities for Contingency Planning:

SPECIFIC REQUIREMENTS
PLANNING
PREPARATION OF PLANS
<ul style="list-style-type: none"> ● Establish review of needs across organisation. ● Identify location of centralised facility and secure agreements across other units. ● Where necessary develop additional marginal resources e.g. mobile towers.
FAIL TO SAFE
Phase 1: Immediate Actions
<ul style="list-style-type: none"> ● Inform other users of a centralised facility of a potential incident (they may lose their backup cover). ● Take initial steps to reconfigure the centralised facility. ● Consider use of centralised facility in 'clearing the skies' if a 'hot swap' is possible. ● Consider potential incidents involving contingency facility by identifying lead unit for secondary contingency.
Phase 2: Short/Medium-Term Actions
<ul style="list-style-type: none"> ● Complete configuration of the centralised facilities. ● Initiate contingency for security/facilities management etc at the centralised site. ● Depending on contingency, plan for gradual hand-over to centralised facility (flight plan, radar, communications etc). ● Identify key staff to be moved from failing unit and possibly from other eligible units to centralised facility.
SERVICE CONTINUITY
Phase 3: Relocation
<ul style="list-style-type: none"> ● Initiate relocation plan for Operational and System support staff - some staff, however, may already be available at Centralised facility. ● Sectorisation changes may be needed if centralised facilities have less working positions/resources available than primary site. ● Ensure systems team validate reliability of data and communications infrastructure not just as Centralised facility goes live but also during initial operation. ● Secure lines of command and management by only allowing necessary staff to travel to Centralised site. ● Remaining staff stay at failing unit to secure recovery.
Phase 4: Optimisation at Central Unit
<ul style="list-style-type: none"> ● Bring in additional staff to ensure adequate rest and rotation of watches. ● Training of additional staff on Centralised facility to aid shift rotation etc.
RECOVERY
Phase 5: Longer-Term Response & Recovery
<ul style="list-style-type: none"> ● Review impact of contingency plans on other units as well as failing centre in terms of safety, security and operational performance.

Figure 8: Case Study of a Solution using Centralised (national) facilities for Contingency Planning

The Strengths, Weaknesses, Opportunities and Threats associated with a Centralised (National) strategy for Contingency planning are shown below:

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● Possibly a reduction in overall costs and resources when compared with an alternative strategy of providing individual contingency facilities for all other national sites operated by a service provider. ● If the principle of 'minimal differences' is applied, (between an ANSP's units and Centralised centre) then there should be no major training, process and procedures issues. ● Simplified logistics and management; equipment economies of scale possible if common systems adopted. ● Centralised centre could provide a corporate focus for resources and training. ● No need for international agreements (LoAs). ● Offers the possibility of recruiting additional Operational and Engineering System staff (including contractors) from other units to support staff both at the Centralised contingency facility and at a failing unit. 	<ul style="list-style-type: none"> ● Significant overheads to ensure that the single national contingency centre keeps pace with changes in all of the other national sites. ● Relocation can be problematic if staff are unwilling to move. ● Relocation would be particularly difficult under pandemic conditions or in the aftermath of terrorist attacks. ● May also be a problem to persuade key staff to stay behind at the failing unit rather than rushing off to set up the alternate facility. ● As a technical solution Centralisation addresses the N-1 scenario but does not adequately address N-2 secondary redundancy issues. ● Unrealistic expectations about scenarios covered by contingency centre.
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● Provides a resilient approach with the potential for State backing where significant security risks exist. 	<ul style="list-style-type: none"> ● Possible internal social and politics concerns may arise within ANSPs if the central site can take over responsibility for their traffic under contingency operations: <ul style="list-style-type: none"> ● <i>Social concerns: employees in other sites may feel threatened in their activity.</i> ● <i>Political concerns about the status of neighbouring centres.</i> ● These concerns should be solved by social dialogue. ● Developing national contingency centres could be difficult to sustain if seen to undermine the advance and facilitation of FAB and SESAR concepts and objectives.

Figure 9: SWOT Analysis for Centralised (national) Facilities for Contingency Planning.

2.5 ATS DELEGATION (INTERNATIONAL) - (CROSS BORDER)

Air Traffic Services can be delegated to neighbouring countries for them to take over some elements of a failing unit's workload as supported by international agreement (e.g. Letter of Agreement-LoA).

The ATS Delegation strategy described below conforms in some aspects with the advice provided in the main "Guidelines" at Appendix C - Alternate Airspace Strategies. The standard contents, relevant to contingency provisions, to be included in an International Agreement (e.g. LoA4) can also be found in the "Guidelines" in Appendix F.

GENERAL CHARACTERISTICS

- The planning phase must focus on establishing political, managerial and technical consensus to be embodied within an International agreement.
- There is greater emphasis to rehearse the contingency provisions in LoA to ensure that they can be acted upon when the need arises.
- During the Immediate Actions phase, neighbouring units must be alerted to the potential for a contingency.
- The Immediate Actions must be agreed between the two (or more) ANSPs.
 - *Should the skies of the failing unit be cleared or should some form of service provision be shared across the failing and the aiding unit - assuming that the aiding unit can re-route traffic into the failing unit's national air space?*

- *As per ICAO Annex 11, there is an underlying assumption that there will be no agreement to enable another ANSP to control the national airspace of another service provider.*
- *Includes the hand-over of traffic from the failing unit - assuming that this is possible using secondary and back-up systems.*

- All aircraft must be accounted for - previous incidents have shown that some traffic may not be informed of a contingency given the stress and high workloads that characterise these situations.
- Detailed discussions are needed to confirm any routing and loading changes.
- Controller licensing requirements at aiding units must be cleared with Regulators/NSAs (as agreed) of both States beforehand.
- Workload may be redistributed in consultation with the CFMU and neighbouring states in order to optimise any residual capacity in the failing unit and, for example, to minimise disruption to over-flights.
- In the context of the Maintenance stage, there is a need to feedback any lessons learned into the planning process. This is likely to lead to revisions to LoAs and to the technical/managerial annex that is associated with any high-level international agreement.
- It may also be necessary to include third parties in such a revision depending on the knock-on effects that were observed during the contingency event.
- Provision of ANS contingency measures over the 'High Seas' areas remains the responsibility of the

State(s) normally responsible for ANS provision.

- *Approval of the contingency plan by ICAO is required - see Appendix C - Alternate Airspace Strategies in the "Guidelines".*

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of using ATS Delegation (International/ Cross Border) for Contingency:

SPECIFIC REQUIREMENTS
PLANNING
PREPARATION OF PLANS
<ul style="list-style-type: none"> ● Establish political and regulatory support for ATS Delegation approach supported by LoAs. <i>In such case, early engagement with Regulator/NSA is essential to clarify any international regulatory issues</i> ● Identify technical extent of any support. ● Develop list of contacts and shared procedures. ● Practice hand-overs under contingency to neighbouring units.
FAIL TO SAFE
Phase 1: Immediate Actions
<ul style="list-style-type: none"> ● Alert all neighbouring units under conditions in letters of agreement and obtain political support if necessary. ● The aiding unit must confirm initial report from failing unit and secure political/managerial approval for response. ● Decide immediate actions: e.g. 'clear the skies' or to allow some services to continue while situation is being assessed. ● Alert other agencies including CFMU of potential contingency and changes in regional traffic between neighbouring States.
Phase 2: Short/Medium-Term Actions
<ul style="list-style-type: none"> ● Begin hand-over from failing unit to neighbouring States' facilities. ● OPS in failing unit must verify that all aircraft are accounted for. ● Consider residual services to military and government aircraft that may be maintained even under immediate decision to 'clear the skies'. ● Hold further discussions with CFMU and neighbours to determine medium term flow control.
SERVICE CONTINUITY
Phase 3: Relocation
<ul style="list-style-type: none"> ● It is assumed that there will be no staff relocation under this strategy; however, the following issues should be considered: ● Sectorisation changes may be needed if neighbours cannot replicate facilities and coverage of failing unit. ● SYS teams focus almost exclusively on diagnosis of problem and remedial actions to restore failing unit and ease load on neighbouring ANSP.
Phase 4: Optimisation of ATS Delegation
<ul style="list-style-type: none"> ● Allocate any residual capacity in the failing unit - e.g. to emergency flights. ● Some of the load on neighbouring ANSPs might be taken on by other regional units in the ANSP operating the failed unit.
RECOVERY
Phase 5: Longer-term Response and Recovery
<ul style="list-style-type: none"> ● Identify protocol and timescale for handing back to failed unit.
MAINTENANCE OF PLANS
<ul style="list-style-type: none"> ● Re-draft letter of agreement or the technical annex as necessary. ● Review impact of contingency plans on regional units in both States and third parties in terms of safety, security and operational performance.

Figure 10: Case Study using ATS Delegation (International/ Cross Border) for Contingency

The Strengths, Weaknesses, Opportunities and Threats associated with a ATS Delegation strategy for Contingency planning are shown below:

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● A relatively low cost means of maximising existing resources. 	<ul style="list-style-type: none"> ● States reluctant to 'hand over' national sovereignty. ● Sensitivities concerning security and air policing activities, e.g. dealing with 'renegade' situations would need careful coordination. States may be reluctant to cede control of such incidents to other States. ● Difficulties exist in ensuring the practical and technical high-level aims and ambitions in a LoA actually mean anything in practice. <ul style="list-style-type: none"> ● <i>LoAs are often little more than statements of intention and lack detail that is necessary in contingency situations.</i> ● <i>Hard to know what can be achieved with different SOPs/equipment etc.</i> ● Susceptible to seasonal variations: may be workable in low capacity situations but less robust in high intensity periods. ● May restrict aiding unit's existing capacity and/or redundancy. ● Limited duration. Aiding units unlikely to be able to sustain contingency operations in the medium to long term. ● In the Planning stage, cross-border arrangements increase complexity and the range of people to be involved and are likely to include both national regulators and possibly political representatives. ● Controller licensing requirements at aiding units must be cleared with Regulators/NSAs (as agreed) of both States beforehand. ● International insurance and liability issues may preclude this strategy as a viable option.
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● Development of ATS delegation practices, procedures and processes may provide synergies in the move towards FAB and SESAR concepts and objectives. 	<ul style="list-style-type: none"> ● Subject to internal and national political pressures. ● If a neighbour(s) can handle contingency they might bid for a failing unit's traffic on a permanent basis. <ul style="list-style-type: none"> ● <i>Airspace users may also decide to re-route their operations through the neighbouring State if the disruption continues, leading to loss of revenue.</i> ● Since controllers are unlikely to relocate this may create problems in the medium to long-term given that large numbers of them may remain under employed in the failing unit until it is brought back on-line. ● Political distrust between neighbouring States in some regions makes this strategy not viable.

Figure11: SWOT Analysis of ATS Delegation (International/Cross Border) strategy for Contingency Planning.

2.6 SHARED COMMON SYSTEMS (INTERNATIONAL) - (CONTINGENCY CENTRES/OTHER CENTRES IN ADJACENT STATES)

Several States in the same region (e.g. in the context of a FAB) may share a common but dedicated contingency facility. This may be a purpose built stand alone facility or alternatively, an agreement that one (existing) facility in a nominated State will act as the contingency facility for all participating States. Alternatively, it may be more realistic for ANSPs to agree amongst themselves combinations of pairs or groupings based around shared/common systems (e.g. FDPS) to satisfy their contingency needs although it is likely that data and sectorisation will be different. *Reference can also be made to the "Guidelines", Appendix C - Moving Personnel to other Facilities in Adjacent States (Common Contingency Centre).*

Note: *This strategy may appear prospective and is not necessarily reflected in "Current Practice". However, it is certainly one of the most promising scenarios for the mid-term in the context of FABs that are under active discussions amongst different groupings across Europe.*

GENERAL CHARACTERISTICS

- The planning phase must focus on establishing political, managerial and technical consensus to be embodied within an International agreement.
- Ideally there should be minimal differences in the systems (e.g. HMI) between potential Aiding units/shared common site and the primary system that is failing.

- It should be possible to reconfigure the Aiding Units/shared common site so that it is ready to pick up the flow of traffic within a minimum period after any disruption.
 - *Radar and communications infrastructure must be patched to a shared contingency control facility.*
 - *Flight planning data and other data must also be transferred.*
- A staff relocation strategy will be required.
- Prolonged "relocation/detachment of staff" may raise social issues and should be anticipated by social dialogue with unions.
- Need to obtain approval from regulator(s) or State authority for procedures and practices that affect the airspace of the failing unit.
 - *If controllers implementing those procedures are operating from within the borders of another member State.*
 - *Licensing and training issues must be clarified beforehand.*
- Other participating ANSPs/States must be informed once an Aiding unit or the shared common centre is activated.
- It will also be important to consider the transfer of staff back to the failing unit when 'normal operations' are ready to be resumed.
 - *Consideration should be made for what would happen if there were problems during the transfer and the original unit could not be brought back - in this case sufficient staff should remain in the shared location to recover from the failure to resume services*
- Feedback loop essential to ensure that the lessons learned from any contingency or adverse event inform the maintenance of any regional contingency centre shared between participating states.

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of a Shared Common Systems Solution for Contingency Planning:

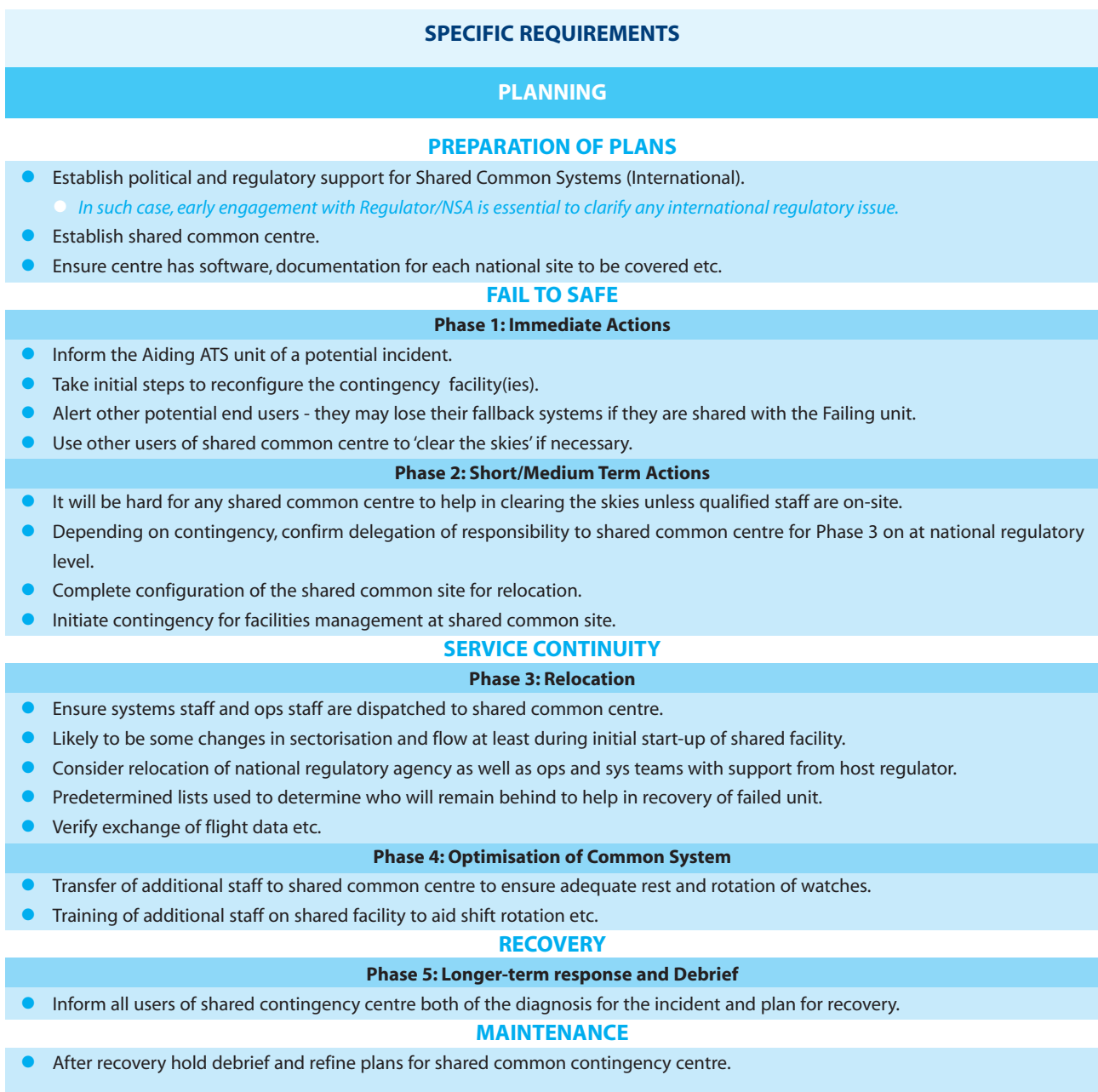


Figure 12: Case Study of a Shared Common Systems Solution to Key Stages of Contingency Planning

The Strengths, Weaknesses, Opportunities and Threats associated with a Shared Common Systems strategy for contingency planning are shown below:

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● Initial and ongoing costs can be shared by participating organisations. ● Avoids some of the problems associated with another State's primary site/aiding unit providing the services of an ANSP using their existing capacity. ● Additional resources imply better levels of technical provision of the shared facility. ● Encourages international cooperation between States and gets focus on contingency ops. ● Transparency and commonality will enhance safety if all participants are 'talking the same language'. ● A shared common facility might also be a mitigation strategy against potential terrorist activity. 	<ul style="list-style-type: none"> ● High continuous (variable) costs in order to ensure that the infrastructure (hardware/software) can be configured to meet the needs of all participating States. ● No standard methodology to determine how to pay for these shared facilities - by traffic volume or equal split between States? ● Some States have diverse traffic patterns (e.g. UK); one shared centre may not be sufficiently flexible to cope with changing demands, e.g. changes in airspace structures etc. ● Staff (controllers and systems engineers) may have to be divided between the failing unit and the facilities that are provided at the shared site. ● Once activated, other States may lose access to their contingency site. ● The strategy is only practical if the ANSPs that contribute to, and rely on, the shared facility also operate very similar systems and practices. ● Additional training will be required if systems, procedures and processes are not similar to those of participating States. ● Legal issues (e.g. licensing and validation) are very complex and need to be overcome for controllers operating in countries other than their own. ● Relocation strategies may be unpopular with staff. ● If one State is using contingency facility then what happens if another also has problems? (Solves N-1 but not N-2)
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● Development of shared facilities, practices, procedures and processes may provide synergies in the move towards FAB and SESAR concepts and objectives. 	<ul style="list-style-type: none"> ● Ability of shared/common facility may be perceived as a threat by national controllers/ANSPs. ● States may want to retain sovereignty and control of backup facilities or control the common system centre - political and security considerations should be taken into account. ● Security and air policing activities are especially sensitive, e.g. dealing with 'renegade' situations would need careful coordination during contingency operations. ● A unilateral upgrade of system etc by one of the participating States may undermine the commonality approach. ● Participating organisations should be committed to long-term funding of the shared facility ● Some States may be more vulnerable to terrorist attack than others.

Figure 13: SWOT Analysis of Shared Common Systems Solution to Key Stages for Contingency Planning.

2.7 HYBRID MODELS

It is possible to identify mixed approaches to contingency. In practice, Hybrid strategies are the most widespread amongst ANSPs. One of the site visits identified a central facility that was being developed to support ATM service provision and at the same time the ANSP was also drafting LoAs with other adjacent States. The same provider was also in negotiation to establish a shared common centre that would be shared amongst all States that operated similar

software. It is impossible to develop detailed case studies for each of the possible hybrid solutions. The additional complexity would also undermine the generic nature of the contingency planning "Guidelines" given that the previous strategies provide a summary at the level of detail that has been included in two previous contingency plans published by ECAC States.

The key point is that the range of security threats and safety hazards facing ANSPs suggests that service providers should

consider a range of possible solutions as per Appendix C in the EUROCONTROL Guidelines.

GENERAL CHARACTERISTICS

- Mix of all other strategies; most widespread.
- Flexible and adaptable.
- May offer greater flexibility for both safety and service continuity.

SWOT ANALYSIS	
STRENGTHS	WEAKNESSES
<ul style="list-style-type: none"> ● Depending on the mix of options taken, then financial costs could be reduced when compared with taking a single option. ● Flexible pragmatic approach. ● Allows international participation but does not rely entirely on LoAs etc. ● Could provide 'defences in depth' (e.g. solving the N-1 N-2 problem), e.g. - use local site as primary contingency and if that fails use a shared common system solution? ● Inherent strengths from other strategies. 	<ul style="list-style-type: none"> ● There is likely to be a lack of political will to fund more than one contingency strategy. ● Multiple contingency strategies could be labour intensive and therefore incur considerable managerial and/or organisational costs. ● Inherent weaknesses of other strategies. ● Complexity to define when to use the right resource/strategy; who use what and when?
OPPORTUNITIES	THREATS
<ul style="list-style-type: none"> ● Even if significant investments have been made in a particular strategy, for example through the development of a national centre for contingency provision, there will be opportunities to consider alternate approaches. ● In the future, with plans for the development of FABs, shared common solutions may become increasingly attractive as ANSPs perhaps seek to share the costs of contingency provision with neighbouring states. ● If the mix of options taken includes shared facilities, practices, procedures and processes then it may provide synergies in the move towards FAB and SESAR concepts and objectives. 	<ul style="list-style-type: none"> ● The choice of selecting purely local solutions (with no international involvement) might undermine cross-border or shared approaches including the move towards FAB and SESAR concepts and objectives.

Figure 14: SWOT Analysis of Hybrid Models for Contingency Planning.

CHAPTER 3. SYSTEMS ENGINEERING PERSPECTIVE ON CONTINGENCY STRATEGIES

Chapter 2 covers some of the broad operational, managerial and organisational actions associated with each contingency strategy. **However, it is also important to stress the critical role played by engineering/technical staff in contingency.** For instance, in the 'Co-Located' and 'Multi-Use' strategies, 're-configuration' of the ATM system is briefly mentioned as a key systems engineering enabler during the Short/Medium Term Actions and/or Relocation Phases. **Indeed, in some cases the ANSPs' underlying approaches relating to systems engineering are likely to have a strong influence on the selection of ANSPs' overall contingency strategy(ies).** This section elaborates the essential contribution of air traffic services engineering personnel during contingency and describes how various engineering approaches affect contingency planning.

3.1 DIFFERENT ENGINEERING APPROACHES

The main Engineering support approaches identified during site visits to ANSPs are:

- In-House Engineering.
- Contractors and Sub-contractors.
- 'Commercial Off the Shelf' (COTS) Approaches.
- Technical (International) Letters of Agreement.

These approaches are NOT mutually exclusive and any single ANSP is likely to have a mix of each. Some ANSPs rely heavily on out-sourcing for key infrastructure items including both hardware and

software applications. Others retain a significant software development function so that they both develop and maintain most of their applications:

Lessons learned collected during visits identified the potential risks of each engineering approach and how these might affect the ability of ANSPs to execute their chosen contingency strategy(ies). These risks and actions to mitigate them are listed hereafter.

3.2 'IN-HOUSE' ENGINEERING

This strategy is currently adopted by a large number of ANSPs.

MAIN CHARACTERISTICS

- Specific solutions are tailored for local needs.
 - *This limits opportunities for 'commercial off the shelf' solutions.*
- ANSPs retain considerable internal resources for the development and maintenance of their ATM systems infrastructures.

POTENTIAL RISKS FOR CONTINGENCY

- Systems engineering teams rely on a relatively small number of individuals with the greatest experience and expertise of primary technical systems.
- Limited number (e.g. one or two) of individuals that have the competencies required to support the transfer of systems infrastructure to a contingency site.
- Potential vulnerability, re core technical staff, for some contingencies related to staff availability (e.g. sickness, terrorist attacks, pandemics).

MITIGATION ACTIONS

During Planning phase:

- Identify potential vulnerabilities and systems skills shortages
- Define proper solutions to deal with staff shortage (including technical/engineering personnel) in case of staff related contingency scenarios (e.g. sickness, pandemics, industrial action, major security breaches).
- In addition, address carefully the impact on "engineering support" capability of core technical experts being absent from the ANSP site, leaving the company or retiring.

3.3 CONTRACTORS AND SUB-CONTRACTORS

The increasing complexity of many ATM systems often prevents ANSPs from maintaining specialist expertise in the development and maintenance of all of the applications that they rely on. Consequently, ANSPs may outsource to contractors the maintenance of their systems. This approach creates specific demands on support of contingency.

MAIN CHARACTERISTICS

- Complex CNS or ATM systems or sub-systems.
- ANSP outsource development and maintenance expertise to external contractors.
- Contractors may be required to support contingency operations (emergency, degraded modes of operation and service continuity).

POTENTIAL RISKS FOR CONTINGENCY

- Support of contractors during contingency operations is out of managerial control of ANSP;
- Contractors' engineering support (efficacy, timing etc) may be insufficient to meet contingency requirements.
- Contractors' reliance on sub-contractors can bring increased complexity and risk.
- It is extremely difficult to envisage the range of constraints that might affect the ability of external agencies to meet contingency requirements, for example during pandemics or major breaches in security.

MITIGATION ACTIONS

During Planning phase:

- ANSPs should ensure that external agencies satisfy the requirements created by particular contingencies.
- External engineering support should be formalised through contractual instruments (e.g. warranties and service level agreements).
- Such agreements should explicit quality and level of engineering support to be provided by external contractors in case of particular contingencies.
- Involvement of sub-contractors to support contractors should be clarified; requirements should be cascaded down to sub-contractors.
- Hold joint drills and exercises with contractors and sub-contractors, especially where contract staff have to be transferred from other projects and sites to help ANSPs respond to a contingency.
 - *Experience in contingency planning within ECAC states has shown that the contractor/sub-contractor relationship can create many*

detailed problems that are only seen during full and partial exercises.

- Clarify ANSPs lines of decision-making up to sub-contractors level:
 - *For example, sub-contractors can find it difficult to identify individual managers with the authority to take critical engineering decisions in the immediate aftermath of a major systems failure.*
- Address carefully scenarios affecting availability of external staff such as major breaches in security or pandemics.
- Address carefully availability of external engineering support in scenarios considering movement of ATCO staff to another site within or out of the State of origin.

3.4 'COMMERCIAL OFF THE SHELF' (COTS) APPROACHES

More and more CNS/ATM systems include COTS elements. This trend will increase in the future with the current developments on inter-operability, development of product by ATM manufacturers. This will continue in the context of SESAR under the pressure of standardisation and inter-operability.

MAIN CHARACTERISTICS

- Several elements of ATM systems and CNS infrastructure are COTS.
- Use of COTS limit direct access of ANSP engineering staff to equipment (hardware and/or software):
 - *There may only be limited opportunities for ANSP engineers to directly access the underlying code for both technical and commercial reasons, for example, real time operating systems.*

POTENTIAL RISKS FOR CONTINGENCY

- ANSP support engineering staff may be prevented from required actions on hardware/software during contingency operations:
 - *e.g. Engineering staff do not have direct access to hardware and or software for repairing and/or debugging.*
- During crisis/contingency, pressing need to contact vendor for intervention on site and/or recruiting expertise at short notice to supplement in-house engineering resources.
 - *This can create considerable problems where, for example, some knowledge of ATM operations may be required in addition to skills in operating COTS applications.*

MITIGATION ACTIONS

During Planning phase:

- Maintain continued agreement between ANSP and vendor on engineering support;
- Define precisely with COTS vendor (or other third party):
 - *Which level and quality of support provided: type of support, reaction times, replacement times, time to repair.*
 - *Which availability (e.g. H24? Weekend?)*
 - *Which stock of back-up supplies?*

3.5 TECHNICAL (INTERNATIONAL) LETTERS OF AGREEMENT

Several European states operate the same core technical systems, which have been tailored for their particular operational needs. This may be particularly appropriate under FAB (and later within the SESAR context).

MAIN CHARACTERISTICS

- International letters of agreement are extended beyond immediate operational requirements to provide wider systems support.
- Systems engineers from one ANSP may be sent to help those of a failing unit in another country.

POTENTIAL RISKS FOR CONTINGENCY

- Similarly to the ATCOs licensing and training concerns of international contingency strategies (refer §2.5 ATS delegation & 2.6 international shared common centre), same concerns arise over the legal status, competency and certification of individual support engineers working on the infrastructure of another country.
- It may also not be possible for other ANSPs to provide individuals with the right level of technical expertise in time to help address a contingency in a neighbouring state.

MITIGATION ACTIONS

During Planning phase:

- Address as required the legal status, competency and certification of support engineers provided by other countries.
- Define with neighbouring ANSP,

realistic requirements in terms of support staff availability.

- Do not over estimate the level of expertise that will be provided.
- Do not under estimate the required familiarisation to your operational systems and environment.
- Address carefully logistics aspects (travel, arrival, accommodation, facilities management etc).

After Execution of contingency, within post-event analysis:

- Debrief the 'foreign' engineering support staff before they return home.
- Avoid bad publicity by ensuring that shortcomings are not ignored.
- Revise contingency arrangements accordingly.

3.6 A LIFECYCLE APPROACH TO SYSTEMS ENGINEERING IN CONTINGENCY.

Systems engineering provision for contingency must change during the lifecycle of ATM applications.

As illustrated below:

- Many major systems are initially commissioned from specialist suppliers.
- As the system moves towards initial installation, the ANSP systems engineering teams should gradually be introduced to the underlying architectures and technologies.
- System suppliers and integrators act as external contractors even though they may be spending long periods working on-site with the ANSP.
- Over time internal systems engineering teams are typically trained to take over responsibility for maintaining infrastructure systems from the initial supplier.
- ANSP system engineering gradually also assumes greater control and independence in coordinating the technical response to any contingency.

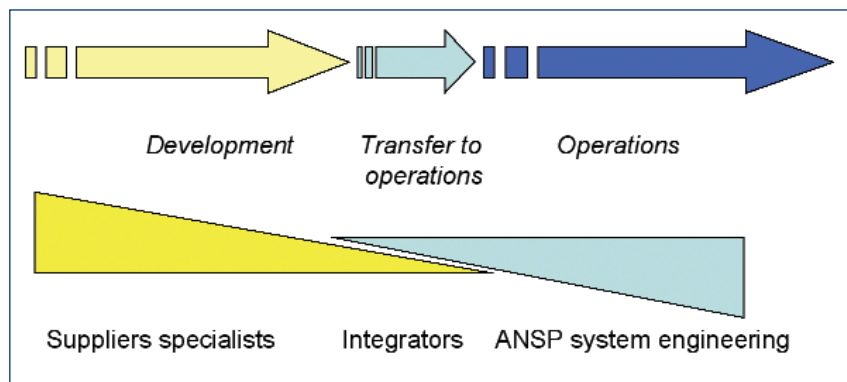


Figure 15: Suppliers and ANSP Engineering staff vis a vis ATM Life Cycle

As changes the initial system are introduced:

- The external supplier may lose the necessary contact with the system as it evolves.
This may jeopardize its capability to be of immediate assistance during any subsequent contingency.
- Therefore, detailed contingency plans should consider both the internal and external staffing requirements for a range of core infrastructures as the identity and nature of these systems will change over time.

3.7 CONCLUSION

Finally, it is important to stress that this section provides only a brief overview.

Each ANSP should ensure that their systems engineering strategy is fully compatible and integrated with their overall approach to contingency.

CHAPTER 4. VULNERABLE SCENARIOS AND COMMON MODE FAILURES

4.1 GENERAL

It is important to stress that the preceding strategies cannot be used to address all possible contingencies. In consequence, alternative plans will have to be made for some of the scenarios that are anticipated when planning for adverse events. Pandemics create particular problems for any plans that involve the movement of staff. It is often necessary to isolate groups of co-workers to help minimize the risks of transmitting the disease. Moving staff from a centre that had already suffered an outbreak might well endanger the health of workers at the aiding unit. Hence, shared regional solutions and centralized facilities that require staff to move from an affected centre would not provide ideal solutions to pandemic contingencies.

4.2 COMMON MODE SCENARIOS

There are a number of other 'common mode' scenarios that might affect both primary and fallback systems under contingency. These need to be considered when selecting between the

different strategies introduced in the previous section. For example, building a contingency facility close to a primary site creates a range of common mode vulnerabilities to flood; power failures; technical infrastructure problems; aircraft accidents; site access problems etc, simply because the two locations are in the same vicinity. If these common mode failures are considered at an early stage then defences can be prepared. For instance, independent power supplies can be installed and UPS backups created to isolate the primary and fallback systems. Pumps and drainage channels can be used to minimize the likelihood that water ingress would affect both the primary and fallback sites at the same time. The cost and complexity of these mitigations should be considered and compared to the substantial savings that can be made by using Co-Located contingency facilities. There are, however, a number of less obvious 'common mode' failures that can affect all contingency strategies. The following sections briefly describe these concerns that were raised during the site visits in this project. Service providers should consider the

threats posed by these common modes of failure as they work on more detailed contingency plans.

4.3 PANDEMICS

A number of European and North American ANSPs have developed contingency plans to deal with pandemics. Pandemics describe epidemics, or an outbreak of an infectious disease, that spreads through the populations across a large region or worldwide. The World Health Organization and European Centre for Disease Prevention and Control provide central resources for planning in this area⁵. They provide several examples of mechanisms that may result in pandemics. They conclude that 'With the increase in global transport and communications, as well as urbanization and overcrowded conditions, epidemics due to the new influenza virus which are likely to quickly take hold around the world'. In order to help organisations plan for pandemics, the WHO have introduced a phased approach.

WHO Phase	Pandemic Period	Characteristics of Phase
Phase 1	Interpandemic period	No new influenza virus subtypes have been detected in humans.
Phase 2		No new influenza virus subtypes have been detected in humans, but an animal variant threatens human disease.
Phase 3	Pandemic alert period	Human infection(s) with a new subtype but no human-to-human spread.
Phase 4		Small cluster(s) with limited localized human-to-human transmission.
Phase 5		Larger cluster(s) but human-to-human spread still localised.
Phase 6	Pandemic period	Pandemic: increased and sustained transmission in general population.

Table 1: WHO Pandemic Phases

⁵ <http://www.who.int/csr/disease/influenza/pandemic/en/> and <http://www.ecdc.eu.int/>

Recent concerns have focused on two particular variants of the influenza virus. In 2003, there were fears that Severe Acute Respiratory Syndrome (SARS) might become pandemic. Rapid action by national and international health authorities helped slow transmission. The disease has not been eradicated, however, and could re-emerge unexpectedly. In February 2004, the H5N1 strain of the

avian influenza virus was detected in birds in Vietnam. This increased fears that the avian influenza virus might combine with a human influenza virus (in a bird or a human) to create a sub-type that was both highly contagious and highly lethal in humans. At present this has not happened and the avian influenza strain remains very inefficient in terms of human to human transmission.

Concerns over the potential threats posed by SARS and H5N1 have prompted several ANSPs to develop specialist plans for dealing with pandemics. These plans are, typically, structured around the WHO Pandemic phases that were introduced in the previous paragraphs. Table 2 illustrates some of the key considerations in the Pandemic plans developed by one European and one North American ANSP.

WHO Phase	Pandemic Period	Characteristics of Phase	Considerations for ANSP Contingency Plans
Phase 1	Interpandemic period	No new influenza virus subtypes have been detected in humans.	Normal operation.
Phase 2		No new influenza virus subtypes have been detected in humans, but an animal variant threatens human disease.	Normal operation.
Phase 3	Pandemic alert period	Human infection(s) with a new subtype but no human-to-human spread.	Traffic will be unrestricted and normal operation should be maintained. However, preparations will be made to identify staff necessary for contingency and possible isolation in subsequent phases.
Phase 4		Small cluster(s) with limited localized human-to-human transmission.	Normal operation will continue unless a cluster appears within the State in question and affects an airport or other ANSP facility. In which case, all plans associated with phase 5 will be activated 'as if the small cluster were a large national outbreak'.
Phase 5		Larger cluster(s) but human-to-human spread still localized.	Traffic will be significantly reduced. Nation States and commercial organizations are expected to introduce travel restrictions and leisure traffic will slow. Health checks may be necessary for family members of ANSP employees. Non-essential staff must remain at home. 50-60% of normal traffic flow.
Phase 6	Pandemic period	Pandemic: increased and sustained transmission in general population.	Traffic will be suspended except for health or government related flights. ANSP staff will be confined to their working premises. Support will be confined to active ANSP personnel. The pandemic may last up to 12 weeks but may recur in several waves. Less than 10% of normal traffic flow.
New Phase 7	Recovery Period	Possible further waves of infection but gradual recovery.	As soon as pandemic status is lifted by government, plans will be implemented to resume normal operations including ensuring currency and health of staff returning.

Table 2: ANSP Considerations during WHO Pandemic Phases

Progression from one phase of a pandemic to another also triggers successively more restrictive constraints upon service provision and on traffic flows. Table 2 also includes an additional 'recovery phase' that is not present in the World Health Organisation guidelines but which is included in all of the pandemic plans that were reviewed during this project. This table also illustrates the way in which the international and national response to pandemics will ease the burdens on ANSPs.

Traffic flows are likely to be cut by the travel restrictions that will be established by States as they seek to protect their populations and also by commercial organisations protecting their employees. However, there will be a continuing requirement to sustain service provision for military flights, for health service and for government infrastructure provision. This also implies a continuing need to maintain systems support during the pandemic and to safeguard facilities management issues. This is likely to prove increasingly difficult as sub-contractors including catering are affected by the pandemic.

In addition to the Generic requirements, the following specific ones apply for the different phases in the case of planning for Pandemics (Strategy Neutral)

SPECIFIC REQUIREMENTS
PLANNING
PREPARATION OF PLANS
<ul style="list-style-type: none"> ● Establish pandemic management cell. ● Establish agreements for SYS, OPS and facilities management to move to centre in phases 5 and 6. ● Agree plans with regulators and government to ensure ANSPs informed by national contingency committees. ● Agree plans for over-flights in pandemic.
FAIL TO SAFE
Phase 1: Immediate Actions
<ul style="list-style-type: none"> ● The initiating event will be government declaring a phase 4 or 5 pandemic. ● If staff continue to work and are exposed to rest of population then consider monitoring health of families. ● After declaration of WHO Phase 4 pandemic, flights will gradually be reduced with no expected need to 'clear the skies'.
Phase 2: Short/Medium Term Actions (<48 hrs)
<ul style="list-style-type: none"> ● Proactive decisions will be needed to gather and isolate key staff in major units. ● Training centre and all non-essential facilities will be closed with remote Internet/wireless communications to all homes in place. ● Other staff will be sent home but with plans to maintain currency and medical fitness for return to normal operations. ● Implement international agreements on over-flights during pandemic.
SERVICE CONTINUITY
Phase 3: Relocation
<ul style="list-style-type: none"> ● Military support may be moved to contingency facility if co-located with civil system to increase isolation and containment. ● Otherwise, staff movements will be avoided. ● Specific legal and administrative duties will be supported by staff 'on call' but work to be highly restricted. ● Safety staff will be available to assess risks of reduced operations.
Phase 4: Optimisation
<ul style="list-style-type: none"> ● Corrective maintenance on all units. ● Continue contact with CFMU on optimisation of airspace. ● Electronic means of communication to be used rather than paper based exchanges with opportunities for contamination. ● Cash flow to be secured by finance department. ● Monitor isolation procedures and control disinfection of premises on regular basis.
RECOVERY
Phase 5: Longer-Term Response and Recovery
<ul style="list-style-type: none"> ● Once government has confirmed that pandemic is over, staff will gradually be brought in. ● Staged return reduces vulnerability to further waves in pandemic. ● Consultation with end-users and government on priorities for return to normal operation.
MAINTENANCE
<ul style="list-style-type: none"> ● Revise contingency plans to consider subsequent outbreaks as soon as possible.

Figure 16: Case Study of Planning for Pandemics (Strategy Neutral).

The previous shows how the five phase model for contingency planning in Air Traffic Management can also be used to structure the response to a pandemic. ***There are strong differences between the activities in these plans and those that might be used in other contingencies.*** Instead of supporting relocation to aiding units, the aim is to isolate staff and limit movements that might expose them to the risks of infection. This is not intended to replace the WHO model, illustrated in Table 2 but is included as an alternate perspective and to retain consistency with the preceding strategies. It is important also to note that Figure 7 is strategy neutral. The same concerns could guide and inform the use of different contingency facilities. For example, if an ANSP had developed a centralised fallback centre for use during other adverse events then staff might be brought in to staff this unit during the pandemic. Alternatively, they might be sent to a shared common contingency facility. In such cases, however, there would have to be a good justification for increasing the risks of cross-infection by leaving the normal centres and some steps would have to be taken to ensure the fitness of personnel arriving at the contingency locations.

4.4 SOFTWARE BUGS

The introduction to this section of the report identified 'common mode' failures to be events that might threaten both primary and contingency facilities, irrespective of the strategy chosen in section 2. Pandemics are only one example of such a threat because they have the potential to affect staff across a wide range of different locations. Software bugs create similar vulnerabilities. If the same software systems are

used in the primary applications as are used in secondary and fallback systems then there is a danger that a single bug could cause vulnerabilities throughout contingency systems. This concern would affect Co-Located facilities just as it would regional or national centres.

There are numerous safeguards against such common mode failures. ESARR 6 and its associated guidance material introduce many of these approaches. For instance, N-version programming techniques can ensure that different companies create independent primary and contingency facilities. However, this can be extremely costly and does not, typically, provide protection against failures that stem from problems in configuration data. Other ANSPs use careful version control so that it should always be possible to roll back to a previous working version of a system. However, this can take a considerable amount of time depending on the point at which a bug was originally introduced into an application. A particular concern over this common mode threat is that the increasing integration and complexity of software systems may make these types of problems harder to identify, especially given some of the plans for future airspace configurations in both Europe and North America.

4.5 INTERNAL SECURITY VIOLATIONS

A further form of 'common mode' failure stems from deliberate violations from company employees. Although there is limited evidence for this to have happened in ECAC member States, other ANSPs have been blackmailed by former employees claiming to have introduced bugs and other deliberate flaws into ATM

systems. Such threats are both more insidious and harder to rectify given the degree of inside knowledge that such individuals may possess.

4.6 CONCLUSION ON COMMON MODE FAILURES

It is important to acknowledge that this is a partial review of the common mode failures that can affect both primary systems and contingency provision, irrespective of the contingency strategy listed in Section 2 of this document

The aim is to encourage ANSPs to consider and prepare for the vulnerabilities that will exist in any approach to contingency planning.

REFERENCES

1. EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services, EUROCONTROL - GUID-0104 released October 2007, http://www.eurocontrol.int/ses/gallery/content/public/docs/pdf/tesis/EC_ContingencyGuideMain_LR.pdf
2. Reference Guide to EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services, EUROCONTROL - GUID-0105 released October 2007, http://www.eurocontrol.int/ses/gallery/content/public/docs/pdf/tesis/EC_ContingencyRG_LR-A4.pdf

GLOSSARY

EXPLANATORY NOTES

For the context of this document only, the following terms are used with the following understanding:

CLEAR THE SKIES

Emergency/ immediate measures taken in response to a contingency event designed to provide maximum possible safety assurance for traffic in the affected area of responsibility by the use of remaining or independent back- up/ fall-back systems:

- Executed by the failing unit and/or pilots and neighbouring units depending on the circumstances at the time.
- Dispersal of traffic receiving a service "as they are" (measures may include suspension of FLAS, emergency vertical separation and visual clearances).
- Refusal of 'inbound' traffic from other service providers (internal and external).
- Imposition of strict/nil flow control measures in co-ordination with CFMU.

- Postponing/limiting departing aircraft from aerodromes within the affected area of responsibility.

COMMON FAILURE MODE

A failure that is common to, and therefore might affect, both the primary (failing unit) and contingency (aiding unit) systems - e.g. power supply, software bug.

TERM	DEFINITION
CONTINGENCY - GENERAL	
Contingency Plan	The detailed exposition of all the actions, including their associated timing and responsibilities, to be performed following the declaration of any of the contingency modes shown in the Contingency Life-Cycle.
Contingency Life-Cycle	All potential contingency modes ranging from 'Normal' Operations, 'Emergency' Situations; 'Degraded' Modes of Operation; 'Service Continuity'; 'Recovery to Normal Operations' and back to 'Normal Operations'.
Implementation	The various steps involved in producing a viable contingency plan(s) based on selected strategies and verifying that the detailed preparations are in place that will enable the plan(s) to be executed.
Execution	The physical enactment of the actions and measures detailed in a contingency plan(s) in response to an event that triggers any contingency mode of operation ⁶ .
Requirements	The detailed demands (safety, security, capacity, efficiency and environment) placed on an ANSP by the State Authorities and agreed with Users relating to the expected ANS provision in contingency situations.

TERM	DEFINITION
------	------------

CONTINGENCY MODES (FROM THE CONTINGENCY LIFE-CYCLE)

'Normal' Operations	Routine service provision within a non-significant variation in Quality of Service.
'Emergency' Mode	'Emergency' modes are those situations following unforeseen or sudden catastrophic events that may lead to potential unsafe situations and/or partial or full interruption of the ANS provision, therefore prompting an immediate response to contain the adverse impact and where feasible initiate recovery actions.
Fallback Modes of Operation	Fallback mode is the use of systems or services that provide redundancy/back-up to those available in support of normal operations, to cope with foreseen or unforeseen unavailability or degradation of the main service provision.
Degraded Modes of Operation	A reduced level of service invoked by equipment outage or malfunction, staff shortage or procedures becoming inadequate as a knock-on effect of one or several deficient system elements.
Service Continuity	Service Continuity (SC) is the availability of suitable arrangements allowing alternate ANS services of an agreed quality of service to be readily activated when a long-term disruption of normal service provision is anticipated. SC is also characterized by containing the impact and duration of disruption of ANS-critical services and the ability to restore a defined service level (capacity) with due priority.
Recovery	Transition back to Normal operations from any of the contingency modes of operation.

OUTAGES

Outage/Failure	A state of inability to continue to provide the normal air navigation service at an agreed quality of service.
Disruption of Service	The inability to continue to provide normal air navigation service provision, caused by staff shortage, unlawful interference, equipment failure, natural disasters or any other unforeseen hazards, resulting in a significant loss in air navigation service provision capabilities.

SEVERITY OF OUTAGES

Outage	An exceptional circumstance, foreseen (e.g. pandemics, industrial action) or unforeseen (e.g. security breach), affecting one or more elements of the System (people, procedures & equipment) that, in the absence of adequate fallback arrangements, may lead to service disruption.
Partial Outage	Partial outages are situations where: <ul style="list-style-type: none"> ● A defined portion of the total traffic is serviced by a failing unit and the rest by one or more aiding unit(s). ● A defined number of sectors/groups are still able to continue with the service provision, whilst the remaining sectors/groups are supported by one or more aiding units. ● A defined set of ATS is still provided by the failing unit while the remaining set is provided by one or more aiding unit(s). ● Any combination of the preceding cases.
Total Outage	The providing unit is declared out of service due to a complete inability to provide air navigation services.

TERM	DEFINITION
PREDICTABILITY OF OUTAGES	
Unforeseen Outage	<p>“Unforeseen” outage is a failure that may lead to potential unsafe situations and/or disruption of the ANS provision and either is:</p> <ul style="list-style-type: none"> ● Unforeseen. ● Or predicted but at too short notice to permit the deployment of a suitable contingency mode.
Foreseen Outage	<p>“Foreseen” outage is a failure that may lead to inability to continue with the ANS provision but is foreseen with sufficient notice to permit the deployment of a suitable contingency mode.</p>
DURATION OF OUTAGES	
Short-Term Outages	Outages or disruption of services lasting not more than 48 hrs.
Long-Term Outages	Outages or disruption of services lasting more than 48 hrs.
AIDING / FAILING UNIT	
Aiding Unit	An ATM unit able to provide support to a failing unit.
Failing Unit	ATM unit unable to provide its services due to catastrophic outage or disruption.

ABBREVIATIONS

ABBREVIATION	DEFINITION
ACC	Area Control Centre
AIS	Aeronautical Information Service
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOP	Airport Operator
ASM	Airspace Management
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSP	Air Traffic Service Provider
AUP	Airspace Utilisation Plan
CAA	Civil Aviation Authority
CAC	Centralised Approach Control
CCC	Common Contingency Centre
CBA	Cross Border Area
CEO	Chief Executive Officer
CFLAS	Conflict Free FL Allocation Scheme
CFMU	Central Flow Management Unit
CM	Crisis Management
CMG	Crisis Management Group
CNS	Communication, Navigation and Surveillance
CR	Common Requirements
CRAM	Conditional Route Allocation Message
CTF	Contingency Task Force
DAP/SSH	Safety, Security, Human Factors Division
EC	European Commission - (also used for European Community)
ECAC	European Civil Aviation Conference
ESP	European Safety Programme for ATM
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAB	Functional Airspace Block
FDP	Flight Data Processing
FIR	Flight Information Region
FL	Flight Level
FPL	Flight Plan
GAT	General Air Traffic
HMI	Human Machine Interface
HR	Human Resources
ICAO	International Civil Aviation Organisation
LoA	Letter of Agreement
MET	Meteorological

ABBREVIATION	DEFINITION
MoT	Ministry of Transport
MoU	Memorandum of Understanding
NOTAM	Notice to Airmen
NSA	National Supervisory Authority
OAT	Operational Air Traffic
OLDI	On Line Data Interchange
RA	Risk Assessment
SES	Single European Sky
SESAR	Single European Sky ATM Research
STAR	Standard Arrival Route
TDU	Training Development Unit
TIBA	Traffic Information Broadcasts by Aircraft
TMA	Terminal Manoeuvring Area
TWR	Tower (ATC)
UAC	Upper Area Control Centre
UIR	Upper Information Region
VCS	Voice Communication System

WEBSITE*info*

www.eurocontrol.int/ses/public/standard_page/sk_sesis_guidelines.html

To provide feedback on the use of this material, to get more information on the subject, or to be informed of the next editions of the Guidelines, please contact Mr Gerald Amar, Project manager at: contingency.planning@eurocontrol.int

This document can also be read in conjunction with the "EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services" and the "Reference Guide to EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services" that may also be obtained from the EUROCONTROL Internet or E-mail addresses listed above.

© European Organisation for the Safety of Air Navigation (EUROCONTROL)

February 2008

ISBN Nr - 978-2-87497-012-2

This document is published by EUROCONTROL in the interests of exchange of information.

It may be copied in whole or in part, providing that the copyright notice and disclaimer is included.

The information contained in this document may not be modified without prior written permission from EUROCONTROL.

EUROCONTROL makes no warranty, either implied or expressed, for the information contained in this document, neither does it assume any legal liability or responsibility for the accuracy, completeness or usefulness of this information.

Published by:

EUROCONTROL Headquarters

Directorate of Human Resources and Administration

96, rue de la Fusée

B - 1130 Brussels, Belgium