EUROCONTROL

EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services

(including Service Continuity)

Edition 2.0

EUROCONTROL

DOCUMENT IDENTIFICATION SHEET

TITLE

EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services (including Service Continuity)

PROGRAMME REFERENCE INDEX

- ***ALDA Reference:***
  EUROCONTROL - GUID-0118

DOCUMENT IDENTIFIER

- ***Edition Number:*** Released Issue
- ***Edition Date:*** April 2009

ABSTRACT

The aim of these Guidelines is to provide a framework to assist States/ANSPs to fulfil their obligations to have contingency plans in place and thus be in a position where they will be able to continue to meet Safety, Capacity, Efficiency, Security & Environmental Sustainability requirements. The construction of contingency plans has not only to satisfy local/national requirements but also to serve the wider interests of regional and network (Pan-European) ATS provision. This document should be read in conjunction with the Reference Guide.

KEYWORDS

- Common requirements
- Contingency
- Degraded modes
- Service Continuity
- ICAO
- Emergency
- Service
- State
- NSA
- ANSP
- Airport
- Airspace users

AUTHORS

Gerald Amar

Richard Lawrence

CONTACT(S) PERSON

Gerald Amar, CND/CoE/P&M/SA

Tel: +32 (0)2 729 36 93

Richard Lawrence, CND/CoE/P&M/SA

Tel: +32 (0)2 729 30 29

DOCUMENT STATUS AND TYPE

STATUS

□ Working Draft
□ Draft
□ Proposed Issue
☑ Released Issue

CATEGORY

☑ Executive Task
□ Specialist Task
□ Lower Layer Task

CLASSIFICATION

□ General Public
☑ CND
□ Restricted

ELECTRONIC BACKUP

INTERNAL REFERENCE NAME :

I:\CND\ND\SSHV\SAF\ESP\GEN 01 - Contingency\14. Contingency Guidelines Edition 2.0

DOCUMENT CHANGE RECORD

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

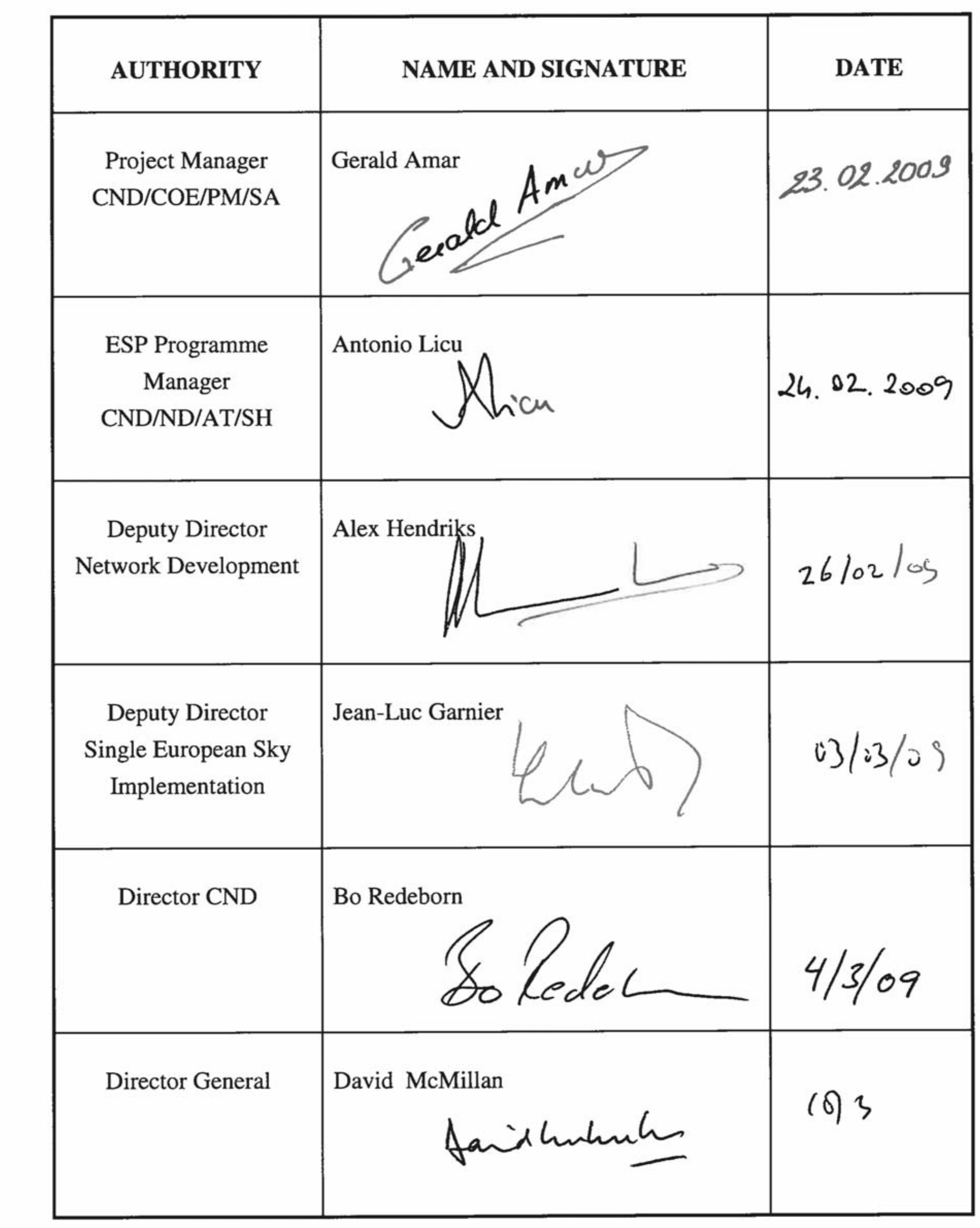
EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
Edition 2.0	06/04/2009	Released issue	All

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

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 CND/COE/PM/SA	Gerald Amar Gerald Amar	23.02.2009
ESP Programme Manager CND/ND/AT/SH	Antonio Licu ALicu	24. 02. 2009
Deputy Director Network Development	Alex Hendriks	26/02/09
Deputy Director Single European Sky Implementation	Jean-Luc Garnier	03/03/09
Director CND	Bo Redeborn Bo Redel	4/3/09
Director General	David McMillan	10/3

ACKNOWLEDGEMENTS

The following list shows the persons that have actively contributed to the production of the Document, in the preparation and the revision phase.

AUTHORITY	NAME
Contingency Task Force Members	Mr Christian Desprets, Belgocontrol, Belgium Mrs Peggy Devestel, Belgocontrol, Belgium Mr Cedomil Svarc, Croatia Control Ltd., Croatia Mr Frank Giraud, DCS, France Mr Claude Miquel, DSNA, France Mrs Elisabeth Lefebvre, DSNA, France Mr Michael Maeding , DFS Deutsche Flugsicherung GmbH, Germany Mr Klaus Dieter Schuette, DFS, Deutsche Flugsicherung GmbH Germany Mr Francesco Di Maio, ENAV SPA, Italy Mr. P. D'Aloia, ENAV SPA, Italy Mr Joao Rodrigues, NAV Portugal EPE, Portugal Mr Milenko Majstorovic, SMATSA, Serbia Mr Bruno Genal, SMATSA, Serbia Mr Peter Barboriak, LPS SR š.p., Slovak Republic Mr Igor Urbanik, LPS SR š.p., Slovak Republic Mr Peder Alber , The LFV Group, Sweden Mr Wim Holthuis, ATC The Netherlands - LVNL, Netherlands Mr Robin Valkenburcht, Ministry of Transport, Netherlands Mr Peter Tormey , Safety Regulation Group (Civil Aviation Authority), United Kingdom Mr Steve Hall, NATS, United Kingdom Mr Daniel Kiper, PANSA, Poland Mr Pascal Latron, Skyguide, Switzerland

AUTHORITY	NAME
EUROCONTROL **Internal Project Team**	Mr Gerald Amar, Project manager Mr Richard Lawrence, Deputy Project manager Mr Antonio Licu, ESP Programme manager Mrs Nathalie Le Cam, Legal expert Mr Patrick Mana, Safety expert Mr Gilles Le Galo, Safety expert Mr Rainer Koeller, Security expert Mr Jean Michel de-Rede, Safety expert Mrs Daniela Grippa, Safety expert Mr Ben Bakker, ATS expert Mr Patrick Delhaise, Communication expert Mr Andrew Taylor, Airport expert Mr Ken Thomas, CFMU expert Mr Cay Boquist, Airspace, Network Capacity & ATM Procedures expert Mr Massimo Bernacconi, CEATS Mr Antonio Nogueras, Civil-Military coordination expert Mr Javier Balsera-Goni, Legal expert Mr Ralf Hendriks, MUAC Support Mr Brian Considine, Training and Licensing expert Mr Andrew Belshaw, ECIP expert Mrs Laura Shapland, EAD expert Mr Wim Janssen, EUROCONTROL Mr Thierry Champougny, Mr Robert Falk, Ms Annika Liindberg, Airspace, Network Capacity & ATM Procedures Simulation experts Mr Bernard Degret, CFMU Simulation tool expert
External Support	Professor Chris Johnson, University of Glasgow Mr Bernard Lucat, Consultant Mr Nicolas, Zveguintzoff, Consultant

LIST OF REFERENCE DOCUMENTS

1. ICAO, Annex 11 to the Convention on International Civil Aviation, Air Traffic Services, Chapter 2.30 and Attachment C, *Material Relating to Contingency Planning*, dated 20 November 2008.

2. Regulation (EC) No 549/2004 of the European Parliament and the Council of 10 March 2004 *laying down the framework for the creation of the single European sky ("the Framework regulation")*.

3. Regulation (EC) No 550/2004 of the European Parliament and the Council of 10 March 2004 *on the provision of air navigation services in the single European sky ("the Service provision regulation")*.

4. Directive 2006/23/EC of the European Parliament and of the Council of 5 April 2006 o*n a Community air traffic controller licence.*

5. Commission Regulation No 2096/2005 of 20 December 2005 *laying down common requirements for the provision of air navigation services (the "Common requirements regulation").*

6. Commission Regulation (EC) No 668/2008 of 15 July 2008 amending Annexes II to V of Regulation (EC) No 2096/2005 *laying down common requirements for the provision of air navigation services, as regards working methods and operating procedures.*

7. EUROCONTROL, *Guidelines for Application of ATS Contingency Planning,* ARR.ET1-GUI-00-00, Edition 1.0, 26 November 1997.

8. EUROCONTROL, Central European Air Traffic Services, *CEATS UAC Operational Contingency Plan - General Principles,* CWP/OPS/AOC/002-Vol…

9. EUROCONTROL, *European Air Traffic Management, Guidance Material Reporting Systems,* Working Draft, Chapters 3-5, SAF.ET1.ST01.1000-GUI-01-00

10. EUROCONTROL, *EUROCONTROL Safety Regulatory Requirement (ESARR) 2, Reporting and Assessment of Safety Occurrences in ATM -* Severity Classification Scheme for Safety Occurrences in ATM, Edition 2.0, 3 November 2000.

11. EUROCONTROL, *EUROCONTROL Safety Regulatory Requirement (ESARR) 3, Use of Safety Management Systems by ATM Service Providers* Edition1.0, 17 July 2000.

12. EUROCONTROL, *EUROCONTROL Safety Regulatory Requirement (ESARR) 4, Risk Assessment and Mitigation in ATM - Safety Assessment Methodology*, Edition 1.0, 5 April 2001.

13. EUROCONTROL, *European Convergence Implementation Programme (ECIP) 2008-2012, GEN 01 "Implement European ANS contingency measures for Safety Critical Modes of Operation"*

14. Business Continuity Institute, Good Practice Guidelines, 2007, *www.thebci.org.*

15. ATM 2000+ Strategy

16. SESAR, *SESAR Definition Phase D3*, DLT-0607-113-00-00 (Security matters)

17. *EUROCONTROL Guidelines for Controller Training in the Handling of Unusual/Emergency Situations.*

18. *Human Factors Module - Critical Incident Stress Management* - HUM.ET.ST13.30000-REP-01 released on 31 December 1997.

19. *Critical Incident Stress Management User Implementation Guidelines* released on 6 December 2005.

20. EUROCONTROL, EATM, *Just Culture Guidance Material for Interfacing with the Media*

21. EUROCONTROL, EATM, *Security Management Handbook,* Edition 1.0, May 2008.

22. EUROCONTROL, EATM, *ATM Security Risk Assessment Methodology,* Edition 1.0, May 2008.

23. EUROCONTROL, EATM, *ICT Security Guidance Material,* Edition 1.0, May 2008.

24. ICAO, *Volcanic Ash Contingency Plan*, EUR Doc 019, First Edition, December 2005.

25. ICAO, *Contingency Planning for Volcanic Eruptions,* Paper by IATA, ATM/AIS/SAR SG/15, 29 July 2005

26. EUROCONTROL, *Air Navigation System Safety Assessment Methodology*, SAF.ET1.ST03.1000-MAN-01, Version: 2.1, 3 October 2006

27. EUROCONTROL, *Safety Case Development Manual,* DAP/SSH/091, Version:2.2, 13 November 2006.

28. EUROCONTROL, *Generic Safety Argument for ATM Safety Assessment,* Version ion 1.1a, , 6 June 2007

29. EUROCONTROL "*A Safe Approach to Transition: Key Elements for Transition Success*", SAM-SSA Chapter 3 - GMD from SAM version 2.2.

30. ICAO Assembly Resolution A36-13, Appendix M - Delimitation of Air Traffic Services (ATS) Airspaces, Associated Practice 2

EUROCONTROL GUIDELINES DISCLAIMER

These EUROCONTROL Guidelines for Contingency planning of Air Navigation Services are 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.

These **EUROCONTROL Guidelines for Contingency planning 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 these guidelines reflects the legislation in force on the date of publication of Commission Regulation (EC) No 2096/2005 in the Official Journal of the European Union, as amended by Commission Regulation (EC) No 668/2008 of 15 July 2008; and of Amendment 46 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.

TABLE OF CONTENTS

TABLE OF FIGURES AND TABLES

NOTE OF THE AUTHOR

"Vision without execution is an hallucination." *Thomas Edison*

In October 2007, EUROCONTROL, supported by a Contingency Planning Task Force (CTF) of Air Navigation Service Providers (ANSPs) and ATM Regulators, published Edition 1.0 of "EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services" aimed primarily at short-term 'Emergency' contingency scenarios.

In early 2008, the Agency also took the first steps to cover longer-term Service Continuity planning by publishing new guidance material to help ANSPs design contingency strategies and operational practices. The "EUROCONTROL Guidance for Design of Contingency Strategies" was made available in February 2008.

However, there was a growing need amongst ANSPs for more in- depth information on Service Continuity issues. In particular more guidance was needed to help ATM Contingency Planning practitioners and their superiors to make more informed decisions on the economic benefits of ATM Contingency Planning. The potential effects of large scale contingency on the European ATM Network as a whole needed to be examined to help inform the economic debate.

Therefore, backed by the Stakeholder Consultation Group (SCG), the CTF embarked on a second phase of work with particular emphasis placed on the economic (business) and safety aspects of long-term contingency planning. To this end a series of ground-breaking simulations was conducted with the aim of providing data to assist in the design of an economic model that contingency practitioners could use to support cost benefit analysis of prospective Service Continuity contingency measures. In the course of the work, further guidance was gathered on the safety, legal, regulatory and security aspects of ATM contingency planning.

The culmination of this work is the production of this second more comprehensive edition of the "EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services" with an improved focus on Service Continuity issues. The main enhancements also include new material on ATM Contingency Policy (Chapter 6) and the introduction of an Operational Concept for ATM Contingency (Chapter 7). The new edition also incorporates at Appendices C and G guidance imported from the "EUROCONTROL Guidance for Design of Contingency Strategies" document. The economic dimension is also strengthened with new guidance (Appendix H) covering some high-level principles for conducting an economic assessment of Contingency Plans for Service Continuity. Enhanced advice for the safety assessment of Service Continuity contingency is provided at Appendix J. Finally, throughout the development work there have been a number of Frequently Asked Questions and these are answered at Appendix K.

The overall objective remains to support ANSPs and State authorities so that the whole ATM community benefits from confirmed best practice and maintains the capability to continue with the provision of air navigation services whatever the circumstances.

To return to the opening quote, the central message is clear: contingency policies, concepts and plans can provide a view of what the situation may look like following a contingency event, but ANSPs **must be ready and prepared to act** in the unfortunate event that they then need to bring these visions into reality.

EXECUTIVE SUMMARY

These EUROCONTROL Guidelines for contingency planning have been prepared under the direction of the Stakeholder Consultation Group (SCG) following its agreement to take ownership of the related ECIP objective in March 2007. A Contingency Planning Task Force (CTF) composed of experts from EUROCONTROL member states was formed to steer development of the guidelines and ensure that they are fit for purpose.

The guidelines recognise that the States and ANSPs responsible for providing ANS are also responsible, in the event of disruption of those services, for instituting measures to safeguard the provision of safe, orderly and expeditious ANS services as far as is reasonably practicable. While the development of contingency plans is mandatory in line with the Chicago Convention and European Community obligations, their exact content is left to the discretion of the States and their ANSPs.

The Guidelines therefore describe a planning process to help States develop their contingency plans in the context of a framework which covers Policy, Planning, Achievement, Execution & Assurance and Promotion. The Guidelines encourage ANSPs to formulate a policy for Contingency in much the same way they do for issues such as Safety and Security. The roles and responsibilities of key ATM players at State and ANSP level as well as the Users are described alongside the essential consultations that need to take place. The Guidelines are applicable to the complete spectrum of ANS services provided: Air Traffic Service (ATS); Airspace Management (ASM); Air Traffic Flow & Capacity Management (ATFCM); Aeronautical Information Services (AIS); Meteorological Services (MET); and Communication, Navigation & Surveillance (CNS). Airport issues are limited to ATM related 'airside' activities.

The Guidelines have 13 chapters covering all aspects of ATM contingency planning based around the framework. Guidance is provided to cover the safety and service/business continuity aspects of contingency and includes advice on the economic issues that are a key part of the equation. Amplifying guidance is provided in a series of Appendices. The document is therefore designed to help ANSPs (large and small) who wish to conceive and develop contingency plans from an immature baseline to those who may wish only to validate their own planning processes and existing plans against the advice provided.

Moreover, for those who are more familiar with ATM contingency, there is an accompanying Reference Guide (RG) to EUROCONTROL Guidelines for Contingency Planning. The RG describes the contingency planning process through a menu of checklists and graphics.

Chapters 1-2 assist ATM Contingency Planners to understand the essential legal background on the need to develop contingency plans in the context of changes in the ATM system since the previous EUROCONTROL Contingency Planning guidelines were issued in 1997.

Chapter 3 describes a 'Contingency Life Cycle' and provides a list of the essential contingency planning related Terminology used throughout the document. Further terms connecting Contingency with Safety and Security are provided in Appendix L; a list of acronyms is at Appendix M - Acronyms.

Chapter 4 outlines the general scope and structure of the Guidelines and their general applicability across ATM.

Chapter 5 describes the roles and responsibilities of the State, ANSPs and Regulator/National Supervisory Authority (NSA). It also looks at legal, liability and cross-border issues associated with ANS contingency planning.

Chapter 6 brings all of the organisational aspects of ANS contingency planning together. It identifies the actors and groups involved in the contingency planning and contingency execution phases.

Chapter 7 encourages ANSPs to formulate a Policy for contingency planning and introduces the Operational Concept for contingency as a necessary step between an ANSP's Policy and the setting of detailed contingency requirements. The process to derive these and the essential consultations that should take place are also described.

Chapter 8 describes a planning process which may be used by ANSPs to develop contingency measures. Using a combination of text and graphics, it describes a process related to the safety critical modes of operation and then details how service (business) continuity strategies might be planned.

Chapter 9 provides a list of contingency planning issues that need to be considered for the full range of air navigation services. The importance of the engineering/technical system is stressed and detailed perspectives on this key part of the contingency planning process are explored in Appendix G.

Chapter 10 stresses the need for ANSPs to test and validate their contingency plans. It also highlights the need for them to maintain a high level of preparedness to execute their plans.

Chapter 11 provides advice on the execution of contingency plans and the importance of assurance activities such as recording activities and monitoring.

Chapter 12 concentrates on the promotion aspects including contingency culture, dissemination of lessons learnt and continuous improvement.

Chapter 13 sets contingency planning in the overall context of Crisis Management.

CHAPTER 1. FOREWORD

EUROCONTROL Guidance Material on Contingency Planning for Air Traffic Services (ATS) was released under the auspices of the European Air Traffic Control Harmonisation Integration Programme (EATCHIP) in 1997. In response to the considerable political, economic, legal, environmental, operational, safety, security, and technological changes that have taken place since then, Edition 1.0 of these Guidelines was developed during 2007 and released in October 2007. Edition 1.0 concentrated mainly on the safety related issues associated with contingency whereas this Edition 2.0 broadens this horizon to cover 'Service Continuity' and network issues.

There are international (ICAO and EC) and sometimes national obligations for Air Navigation Service Providers (ANSPs) to have contingency plans in place. In addition, the ECIP 2008-12 introduced a new objective (GEN 01) related to the implementation of ANS contingency measures.

The separation of ANSPs from States has introduced new economic factors that need to be considered in the context of contingency plans. In particular the financial situation of many ANSPs has changed dramatically; this Edition 2.0 therefore addresses the financial considerations such as the level of funding for contingency measures. European legislation has also introduced new relationships between ANSPs and their NSAs who have responsibility for the oversight of ANSP activities including contingency planning. The Single European Sky (SES) also places more focus on the importance of the Pan-European network effects associated with contingency planning and the need for harmonisation of operational plans, including those for contingency is greater than ever. Functions which were not yet fully established in 1997 (e.g. CFMU and EAD) are now essential to the day-to-day ANS provision and are pivotal in the context of European ATS contingency planning. Contingency planning for ANS also needs to be re-evaluated in the context of recent world events ranging from security threats to possible pandemics.

It is recognised, however, that not all situations can be foreseen. In addition, no two situations will be the same and so no Emergency or Service Continuity plan can cater for every eventuality. That said, certain common factors can, and must, be prepared for.

ANSPs must be able to deal with unexpected events and it is the ability to respond to these in a safe, orderly manner which provides the overriding rationale for the development of contingency plans rather than the legal obligation to do so. Safety is, and must remain, the number one priority. Therefore, this version of the Guidelines provides assistance to States and ANSPs on the 'Emergency' and 'Degraded Modes of Operation' within the Contingency Planning Life Cycle as well as expanded guidance on 'Service Continuity' issues.

CHAPTER 2. BACKGROUND

2.1 OBLIGATIONS UNDER THE CHICAGO CONVENTION AND EUROPEAN COMMUNITY LAW

The Convention on International Civil Aviation (hereafter referred to as the "Chicago Convention"), Annex 11, Air Traffic Services, Chapter 2.30 (Amendment 46) states inter alia that,"*Air Traffic Services authorities shall develop and promulgate contingency plans for implementation in the event of disruption, or potential disruption, of air traffic services and related supporting services in the airspace for which they are responsible for the provision of such services*". Unless they file differences against this standard, States are bound to comply with it.

This provision is further explained at Attachment C to Annex 11, Chapter 2.30 (Amendment 46) which provides inter alia that, "*contingency plans are intended to provide alternative facilities and services to those provided for in the regional air navigation plan when those facilities and services are temporarily not available. Contingency arrangements are therefore temporary in nature […]*". Attachment C has however only the status of guidance. States are not bound to comply with such material interpretation.

In addition, the Single European Sky (SES) Framework and Service provision regulations paved the way for the Common requirements (CR) regulation . In Annex I, to the CR Regulation,§ 8.2 required that "*At the latest one year after certification, an air navigation service provider shall have in place contingency plans for all the services it provides in the case of events which result in the significant degradation or interruption of its services*". As a result, these plans should be have been completed and ready for possible implementation at the latest by end of 2007 (or by mid- 2008 in cases where an extension of 6 months was granted to the State to complete the ANSP certification process. Furthermore, Annex II, to the CR Regulation ,§ 4 states that a provider of air traffic services shall be able to demonstrate that its working methods and operating procedures are compliant with, in particular, Annex 11 to the Chicago Convention (including all amendments up to No 45).

2.2 EUROCONTROL GUIDELINES - AIMS & PRINCIPLES

Both sets of legislation mentioned above contain obligations for the development of contingency plans, but none defines what the exact content of these plans should be (e.g. type of measures, capacity levels, etc.). The only indications are provided as guidance in Attachment C to Annex 11 of the Chicago Convention and refer to "*alternative facilities and services*". Therefore, while development of the plans is mandatory, their exact content (structure, description, etc.) is left to the discretion of the States and their certificated and designated ANSPs.

A prime purpose of the Guidelines, therefore, is to provide information and processes to help States and ANSPs to identify and decide the operational concepts and associated contingency strategies best suited to meet their needs in certain circumstances.

Thus, the Guidelines aim to provide a framework to assist States and/or ANSPs:

- To fulfil their international obligations to have contingency plans in place and therefore be in a position to continue to meet Safety, Capacity, Efficiency, Security & Environmental Sustainability requirements
- To construct contingency plans to satisfy local/national requirements.

The necessity for ANSPs to have an embedded contingency management policy and associated culture within their organisations and of the need for them to be adequately prepared to deal with contingency situations is also stressed. In this context, it is recognised that it is also impossible to cater for every eventuality and causal factor that might give rise to the need to enact a contingency plan. Similarly, the Guidelines do not enter into details to address all possible disruptions.

The main emphasis is put on possible processes and procedures to be followed by the interested parties when developing their contingency concepts and plans although some guidance is provided on the execution and post-execution phases.

This document is rather meant to constitute a tool-box providing a check-list of all elements to take into consideration when addressing the issue of contingency, while the exact content of the measures is left at the discretion of the interested parties.

[1] Regulation (EC) No 449/2004 of the European Parliament and the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the "Framework regulation"), OJ L 96, 31.03.2004, p.1; Regulation (EC) No 550/2004 of the European Parliament and the Council of 10 March 2004 on the provision of air navigation services in the creation of the single European sky (the "Service provision regulation"), OJ L 96, 31.03.2004, p.10.

[2] Commission regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services (the "Common requirements regulation"), OJ L 335, 21.12.2005, p. 13 as amended by Commission Regulation (EC) No 668/2008 of 15 July 2008, OJ L 188, 16.07.2008, p.5.

2.3 GUIDANCE TO SUPPORT ESSIP OBJECTIVE GEN01 IMPLEMENTATION

The implementation of contingency measures for ANS, reflecting the Annex I § 8.2 of the Common requirements, is addressed in the European Single Sky Implementation (ESSIP) (formerly ECIP), via the Pan-European/Agreed objective GEN 01 "Implement European ANS Contingency Measures for Safety Critical Modes of Operation". This objective addresses the safe and orderly degradation of a service in the event of a contingency situation and its eventual safe recovery, in a strictly controlled manner, to the normal capacity operating situation. This document contains guidance to implement the objective for the concerned modes of operation (Emergency, Degrade Mode and Recovery to Normal Operations).

CHAPTER 3. CONTINGENCY PLANNING TERMINOLOGY AND CONTINGENCY LIFE CYCLE

3.1 CONTINGENCY PLANNING TERMINOLOGY

The following terms covering ATM Contingency Planning, as agreed by the Contingency Planning Task Force, are used throughout this document. Specific terminology relating to Safety and Security but which are often used in the context of Contingency Planning are described in Appendix L. In addition, a list of common acronyms used can also be found at Appendix M - Acronyms

TERM	MEANING
CONTINGENCY - GENERAL	
CONTINGENCY PLAN	The detailed exposition of 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 through, 'Emergency' Situations; 'Degraded' Modes of Operation; 'Service Continuity'; 'Recovery to Normal Operations'.
'NORMAL' OPERATIONS	Routine service provision within a non-significant variation in Quality of Service.
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 .
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.
CONTINGENCY MODES (FROM THE CONTINGENCY LIFE-CYCLE)	
'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.

[3] This term is equivalent to "application" as used in the context of Attachment C to Annex 11, Chapter 2.30.

TERM	MEANING
CONTINGENCY MODES (FROM THE CONTINGENCY LIFE-CYCLE)	
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	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: ● 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	MEANING
PREDICTABILITY OF OUTAGES	
UNFORESEEN OUTAGE	"Unforeseen" outage is a failure that may lead to potential unsafe situations and/or disruption of the ANS provision and either is: ● Unforeseen; ● Or predicted but at too short notice to permit the deployment of a suitable contingency mode.
FORESEEN OUTAGE	"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.
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.
MAXIMUM TOLERABLE PERIOD OF DISRUPTION (MTPD)	It is the maximum period of time an ANSP can tolerate a loss or disruption of any Air Navigation service/function provided.
AIDING / FAILING UNIT	
AIDING UNIT	An ATM unit able to provide support to a failing unit.
FAILING UNIT	A unit, which due to technical or system failure, is forced to suspend the provision of ATS in its Area of Responsibility (AoR) or parts thereof.

3.2 CONTINGENCY LIFE CYCLE

In the context of the ICAO and EC obligations, the concept of contingency can be organised along a "Contingency Life Cycle" composed of the following phases:

- 'Normal' Operations, (see Note 1)
- 'Emergency' Situations;
- 'Degraded' Modes of Operation;
- 'Service Continuity';
- 'Recovery to Normal Operations'
- and (back to) 'Normal Operations'.

The meanings attributed to these terms are described in Paragraph 3. A schematic presentation of the Contingency Life Cycle is presented below.

Notes:

1. *'Normal Operations' is included in the schematic for completeness, but 'Normal Operations' is not classified as a Contingency mode.*
2. *"Outage' is an event that causes a state of inability to continue to provide the normal air navigation service at an agreed quality of service (see Para 3.2).*
3. *The 'Emergency', 'Degraded modes of operation', 'Service Continuity' and "Recovery to Normal operation" modes are described in Para 3.2.*
4. *In Figure 1, the horizontal axis shows the time, the durations of the different phases shown are not representative of the length of those phases. They could be very different from one event to another or from one environment to another*
5. *The outage may lead to a disruption whose the elapsed time is of days or weeks.*

This Life Cycle should not necessarily be understood as a sequence of modes of operation. For instance, in certain circumstances depending on the cause/type of disruption:

- A System (Technical, People and Procedures) working in 'Normal' operation can evolve directly into an "Emergency" situation;
- or a System can deteriorate into a "Degraded mode of operation" that further evolves into an "Emergency" situation;
- or an "Emergency situation" can be followed by a 'Service Continuity' mode of operation;
- or in some situations, it might be necessary to move straight from 'Normal' operation into a 'Service Continuity' mode of operation.

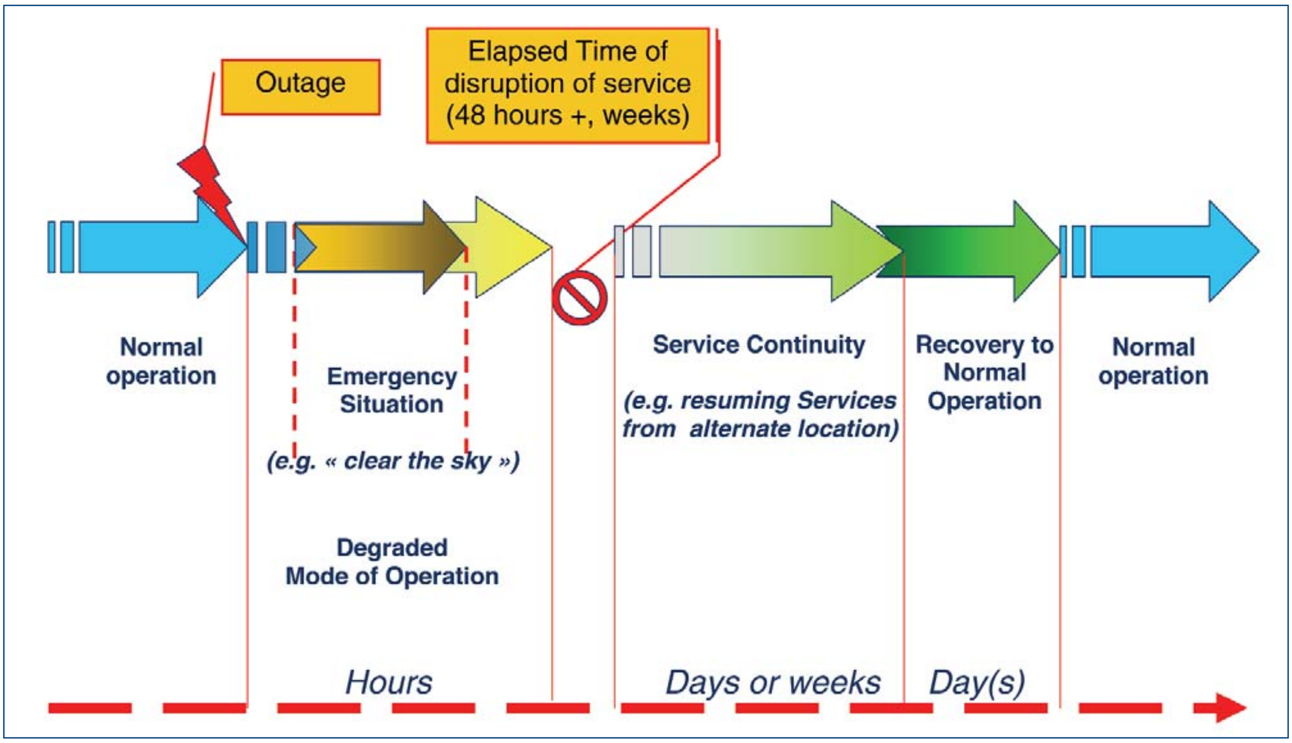

Outage
Elapsed Time of disruption of service (48 hours +, weeks)
Normal operation
Emergency Situation
(e.g. « clear the sky »)
Degraded Mode of Operation
Service Continuity
(e.g. resuming Services from alternate location)
Recovery to Normal Operation
Normal operation
Hours
Days or weeks
Day(s)

Figure 1: Generic Contingency Life-Cycle

3.3 ASPECTS OF CONTINGENCY LIFE CYCLE

The Contingency Life Cycle described previously is at a very high level of abstraction and is largely seen through the aspect of ANS provision in terms of modes of operation. However, it is also possible to view the Life Cycle from a number of other aspects (e.g. Technical, Security and Managerial) to elaborate how outages and other security or crisis events could impact on the provision of ATS and the modes of operation.

3.3.1 TECHNICAL ASPECTS

Within the Life Cycle an outage on the technical side could initiate Fallback modes of operation and ATFM regulations may have to be put in place. Both conditions may last until the outage is fixed. More elaborated guidance can be found in Appendix G - Systems Engineering Perspective on Contingency Strategies.

3.3.2 SECURITY ASPECTS

From the Security aspect a security event could initiate the introduction of specific security measures aimed at safeguarding normal ATS provision. ATFM regulations may also have to be put in place. Both conditions may last until the situation is resolved.

3.3.3 MANAGEMENT ASPECTS

From a Management aspect the Life Cycle can be viewed as the organisation's response to 'crisis' events and subsequent crisis management activities. Depending on their nature, crisis events may also initiate the implementation of ATFM regulations which may last until the crisis is over. Crisis Management is covered further in Chapter 13.

In all aspects, in circumstances where the outage worsens and the situation escalates, it may be necessary to move into a Degraded or Emergency mode of operation. Attempts to restore the failed technical system(s), ameliorate the security situation or re-establish the organisation's overall capabilities will continue to follow as a parallel process. Moreover, depending on the contingency measures in place, technical, security and managerial support of ATS is likely to be required during the Service Continuity and Recovery to Normal Operations phases of the Life Cycle.

3.3.4 EXPANDED CONTINGENCY LIFE CYCLE

The different aspects described above can be represented in an expanded Contingency Life Cycle.

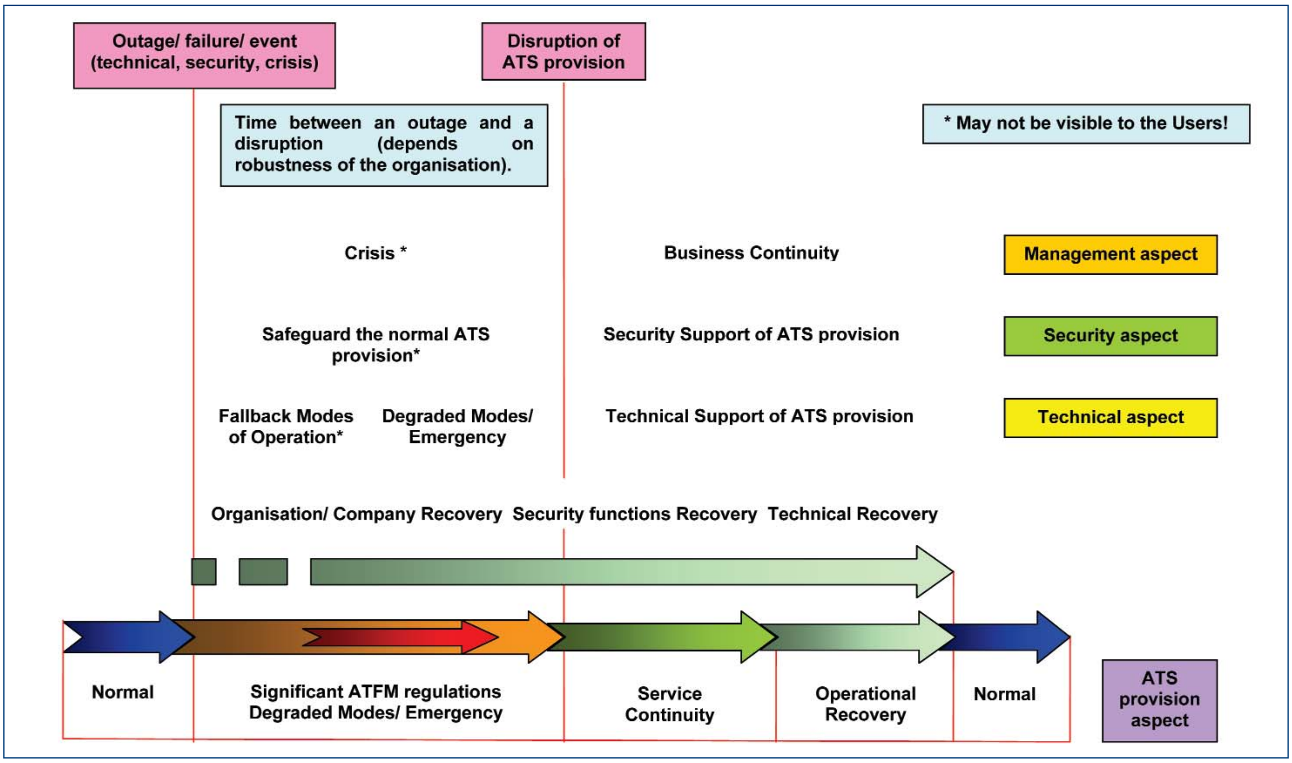

Outage/ failure/ event (technical, security, crisis)
Disruption of ATS provision
Time between an outage and a disruption (depends on robustness of the organisation).
* May not be visible to the Users!
Crisis *
Business Continuity
Management aspect
Safeguard the normal ATS provision*
Security Support of ATS provision
Security aspect
Fallback Modes of Operation*
Degraded Modes/ Emergency
Technical Support of ATS provision
Technical aspect
Organisation/ Company Recovery
Security functions Recovery
Technical Recovery
Normal
Significant ATFM regulations Degraded Modes/ Emergency
Service Continuity
Operational Recovery
Normal
ATS provision aspect

Figure 2: Expanded Contingency Life Cycle

CHAPTER 4. SCOPE AND STRUCTURE OF THE EUROCONTROL GUIDELINES

4.1 GENERAL

This document deals with the planning for ANS contingencies at ANS units. The Guidelines provide advice on how to construct contingency plans for local and national scales of operation and limited advice on regional and Pan-European network level operations. Check lists are provided in the Reference Guide Edition 2.0 to support stakeholders.

4.2 APPLICABILITY OF GUIDELINES

The guidance offered covers the roles and responsibilities of ANSPs and NSAs / Regulators (civil and military) in contingency planning. The ***pivotal role of the CFMU related to the potential network effects of ANS contingency*** is also addressed.

In accordance with the ICAO and EC obligations the Guidelines cover the complete spectrum of ANS services (with certain caveats). As such, all aspects of Air Traffic Control (En-Route/Area Control Centre (ACC), Approach, Tower etc) are considered. In addition, advice is provided for Airspace Management (ASM) and Air Traffic Flow and Capacity Management (ATFCM). Aeronautical Information Services (AIS) and the effects of disruption of EAD on the availability of information flow are taken into account. Contingency of MET services is limited to the information flow which is necessary to provide the required ATS. Similarly, contingency of Communication Navigation and Surveillance (CNS) services, in the scope of these Guidelines, is limited to the supporting services which are necessary to provide the required ATS. However, information is provided on technical and engineering matters that affect Contingency Planning and advice is also provided on issues related to external suppliers (e.g. contractors and subcontractors). For airport operations, the scope is limited to direct ATS at airports and directly associated 'airside' infrastructures such as the control tower buildings and CNS. No 'landside' airport aspects (e.g. baggage handling) are considered although it is recognised that there are many issues here that could impact indirectly the ATS operation.

The Guidelines are primarily intended for use by the civil ANSPs and the military ANSPs (in so far as they have been certified). Non-certified military ANSPs servicing GAT, may find the information useful in the context of developing or updating military contingency plans. However, Contingency measures to be taken in the case of a 'failing' ANS military unit are not specifically addressed in the document, but when developing contingency measures of a civil ANSP, ANS military units might be considered as a possible aid to a 'failing' civil ANS unit.

4.3 LIMIT OF THE GUIDELINES

The accumulative aspects of contingency and “degraded operation” are addressed as far as practicable although it is assumed that when selecting ***mitigating actions and strategies they should have a demonstrably low likelihood of being concurrently affected by another service disruption.***

4.4 GENERAL STRUCTURE

Traditional practices for contingency planning have been based on the identification of the resources available (systems, procedures and staff) and the exploitation of these resources for contingency operations. While this approach has its merits, it also has its shortcomings (e.g. lack of requirements, incomplete consultation of State authorities and airspace users).

To address these issues, a “Contingency Process” framework is introduced that is derived from a classical Safety Management System (SMS) approach: Policy, Planning, Execution & Achievement, Assurance and Promotion. Advice is given on the key contingency planning considerations and activities according to that framework. The high level considerations are provided in the main body of the document whilst the detailed planning needs are addressed in the Appendices.

Briefly, these steps are:

- ***Policy:*** Sets the ANSP organisation's contingency planning policy, operational concept for contingency and establishes the requirements around which the detailed contingency plans will be built (Chapter 7 Policy, Operational Concept and Setting Requirements)
- ***Plan:*** Plan demonstrates how the aims of the set of Requirements that have evolved from the Policy and Operational Concept will be achieved. It also outlines the strategies/actions and resources required. The products of this step are the con-

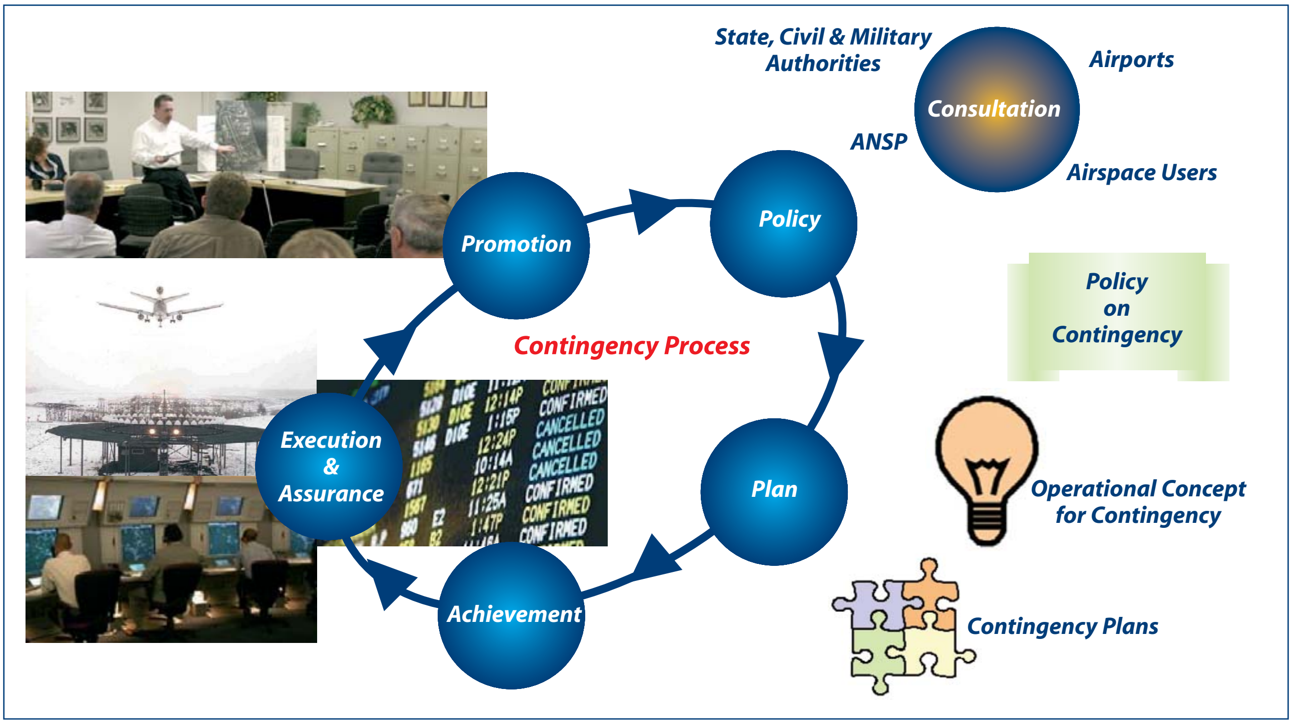


Figure 3: Contingency Process

tingency plan(s) (§ 8.2 Planning Process).

- ***Achievement:*** Achievement verifies that the detailed means for translating the plans into reality are effectively in place. It covers testing, exercising, maintaining and reviewing the various contingency plans and raising awareness of contingency within ANSPs (§ 10).
- ***Execution and Assurance: This step corresponds to the Execution of the contingency plan.*** It includes also the monitoring and recording activities to be undertaken to enable the Promotion (§Chapter 11 Execution and Assurance)).
- ***Promotion:*** Contingency Planning Promotion ensures communication of the contingency culture, dissemination of lessons learnt and enables the continuous improvement of the process (Chapter 12 Promotion).

The arrows forming the loop indicate that ***Assurance*** and ***Promotion*** follow the ***Execution*** of the Contingency Plan and they shall ensure that the Contingency Plan(s) are reviewed and continually improved.

4.5 SPECIFIC CASES

Scenarios such as pandemics, common mode failures and industrial action do not conform in all respects to the 'usual' contingency planning dynamics. Specific advice concerning these scenarios is provided at Annex I.

4.6 CRISIS MANAGEMENT

It is recommended that planning for contingency measures be conducted within the larger framework of “crisis management”. In that context, outline guidance of “crisis management” considerations to help in the development of holistic plans is provided in Chapter 13 Crisis Management The links between the development of contingency plans and crisis management plans are also mentioned in different sections: § 7 (Policy) and Step 6.2 Crisis Management Plans (Planning).

4.7 FREQUENTLY ASKED QUESTIONS

To complement the advice given in the remainder of these Guidelines, Appendix J - Contingency Planning Frequently Asked Question (FAQs) contains a list of questions and answers covering Legal and Regulatory matters, ATM Security and Training, Testing and Exercising.

CHAPTER 5. ROLES AND RESPONSIBILITIES OF STATE, NSA OR ANSP AND LEGAL ASPECTS OF CONTINGENCY

5.1 SCOPE OF THE SERVICES SUBJECT TO CONTINGENCY

While Annex 11 to the Chicago Convention requires contingency plans for air traffic services only (which include flight information service, alerting service, air traffic advisory service and air traffic control service), the SES legislation requires plans for all services provided by "air navigation service providers", i.e. providing ATS, MET, AIS or CNS.

In both cases, the obligation concerns providers of services to general air traffic, which can lead to the conclusion that military providers providing services to general air traffic have also to put in place contingency plans. It should however be noted that the SES regulations apply this obligation only to military providers offering their services primarily to general air traffic.

Article 4 of (EC) Regulation N° 2096/2005 foresees the possibility of limited certificates for ANSPs not providing cross-border services. The limited certificates allow certain derogations to some requirements, such as contingency plans. As a consequence, and subject to meeting the conditions for derogation, not all air navigation service providers are obliged to have in place contingency plans.

5.2 ROLE OF THE STATE

I) POLICY

The role of the States stems from Annex 11 to the Chicago Convention, and in particular from its Chapter 2.30 as interpreted by the guidance of Attachment C.

These provisions are in line with Article 28 of the Chicago Convention, under which States are responsible for providing in their airspace air navigation facilities and services. This responsibility extends to the situations of crisis and to the necessity to maintain where possible the provision of services and a sufficient level of safety.

As a consequence, the State has to prevent, manage and mitigate such situations that would affect the provision of facilities and services by ensuring the prior development of contingency plans by the designated ANSP to whom the services have been delegated.

If the ANSP is an institutionally separated entity (with its own legal personality), the responsibility for the contingency planning will be split between the State and the Service provider. The service provider will be in charge of the development and when necessary the implementation of the plan; the State will remain responsible for approving and promulgating the plan.

In the States where European legislation is applicable (EU States or States having ratified a European Common Aviation Area (ECAA) or other bilateral Agreements), the application of Regulation N° 2096/2005, which requires all ANSPs (and not only air traffic service providers, as provided for in Annex 11 to the Chicago Convention) to have in place contingency plans, does therefore not hamper the responsibility of the States stemming from Annex 11 to the Chicago Convention.

This is confirmed by § 4 of Annex II to Regulation No 2096/2005 referring to the necessary compliance with the Chicago Convention, in particular Annex 11.

II) PLAN

As a consequence, even where the plans are primarily developed by separated service providers, the responsibility of the State remains and is exercised at various levels:

- the State defines, in consultation with interested parties the requirements and targets to met by the contingency plans; in particular the State defines the security aspects to be met by the contingency plans and monitors developments that may lead to events requiring contingency arrangements;
- the State imposes these requirements on the ANSPs either in a law, or a regulation, or on a bilateral basis in the designation act for ATS providers; since AIS and CNS providers are not designated, the requirements will have to be set in legislation/ regulation;
- the State puts in place mechanisms to ensure that the contingency plans are acceptable and in conformity with the defined requirements; for certified ANSPs, the verification of the existence of the plan is done by the NSA (see infra, § 8.1.1.2). The NSA would need to be entrusted with the additional verification of compliance with the requirements. In addition, in application of Article 10 of EC

Regulation No 550/2004, plans involving cooperation of ANSPs for the provision of services would need to be notified to the NSA(s) or approved by the State(s) (in cases involving air traffic services).

- The State ensures the required international relations and co-ordination with other States, where necessary (for instance within functional blocks of airspace), and with international organisations (such as ICAO for the coordination referred to under Note 2 to Chapter 2.30 of Annex 11 to the Chicago Convention). This note indeed provides that contingency plans constituting a temporary deviation from the approved regional air navigation plans are approved as necessary by the President of the ICAO Council on behalf of the Council.

  The effect of service disruption upon international air traffic flows and on the provision of ATS in adjacent airspace can be, depending on duration and circumstances, appreciable. This explains the need for international/ (sub) regional initiatives and co-ordination, involving the CFMU and airspace users. Contingency plans should therefore be prepared, tested and promulgated before the occurrence of events, in consultations with other States and ICAO, as appropriate, preferably at (sub) regional level.
- The State ensures the appropriate communication to the users through the AIS of the application of the contingency plan and of its discontinuation (reactivation of normal services).

III) ACHIEVEMENT

The following actions or elements are part of the role of the State:

- Definition of the requirements and targets for contingency, in consultation with stakeholders; the requirements to be defined by the State include security aspects;
- Inclusion of these requirements / objectives to be met by the ANSPs concerned into a binding document (law, regulation, designation, contract, etc.);
- Entrusting the/an NSA with the verification of the contingency plans;
- Approval of the contingency plans containing delegations of ATS;
- Relations or conclusion of agreements with neighbouring States, for coordination purposes, in particular when the plans include cross-border delegation of ATS and have or would have an effect on the capacity of the neighbouring State;
- Communication of the contingency plans to ICAO at the 'pre-execution' phase depending on the content and intention of the contingency measures;
- Ensure publication of NOTAMs to Users when the contingency plans are applied and discontinued.

5.3 ROLE OF NSA/OVERSIGHT AUTHORITIES

I) POLICY

The State can perform the oversight itself or delegate this task to another entity, through proper instruments. In the States where European legislation applies, the entity in charge of verification of compliance with Regulation No 2096/2005 is the NSA, which has been nominated or established for this purpose. The NSA can also be entrusted, at the discretion of the State, with verification of additional national requirements, e.g. those contained in the designation (for ATS and possibly MET) or in national regulations. Additional requirements related to contingency (for instance capacity levels) as stated in other regulatory documents (for instance in designation act) might therefore be verified.

II) PLAN

The role of the NSA with regard to certification against Regulation No 2096/2005 which is directly applicable in the EU member States should not be restricted to verification of the existence of a contingency plan but should also extend to the verification of its content, its adequacy to the ANSP level of provision. The NSA has to assess for instance that all the services are covered, that the possible cases of disruption are identified, that mitigation measures are in place, that the feasibility is tested and validated, that training is provided, that practical cases are run, and that overall the ANSP is working following the plan.

Regulation No 2096/2005 provides that "*At the latest one year after certification, an air navigation service provider shall have in place contingency plans*". However the correct exercise of the States' responsibilities commends that the content of the plans be in conformity with the requirements they have set and be approved by them. As a consequence, a contingency plan can be valid only if it meets these requirements, and therefore both its existence and its content should be subject to oversight and be conditions for its validity.

[4] The question of the role of ICAO, in particular in relation to High Seas, is further developed in § 9.1.4 as well as in Appendix J (Questions 19 to 21).

[5] The SES Regulations are also applicable in other non-EU States through Agreements (e.g. ECAA)

[6] The present EUROCONTROL Guidelines can be used by the NSAs to define their own specific requirements but do not constitute per se binding acceptable means of compliance.

The NSA has to define in advance, adopt and communicate to the ANSPs concerned, the criteria /requirements against which it will assess the Contingency Plan. This will allow the ANSP to determine what may constitute or not acceptable means of compliance to meet the requirements.

The approval of the contingency plan by the NSA should be part of the certification process and ongoing supervision, and should not be given separately. It can be treated in a specific chapter of the audit report.

If the contingency plan is not approved, the NSA can decide to organise intermediate auditing more frequently and request the ANSP to implement a corrective action plan. If no remedial action is taken, sanctions could be imposed, according to national law.

Finally in application of Article 2.4 of Regulation (EC) No 550/2004, the NSAs have to make appropriate arrangements for close cooperation with each other to ensure adequate supervision of ANSPs providing services in the airspace falling under the responsibility of several States. This cooperation, which may be required if the contingency measures involve cross-border delegations of services or involve ACCs within a FAB, should extend to the handling of non-compliances.

III) ACHIEVEMENT

The following actions or elements are part of the role of the NSA:

- Definition of criteria and procedures for the verification of contingency plans, and communication to the ANSPs concerned
- Verification of the existence, substance and adequacy of the contingency plans, in accordance with Regulation No 2096/2005 as well as with the requirements and targets defined by the State
- Definition, and where appropriate request, for corrective actions in case of non-conformities
- Coordination with other NSAs concerned, particularly in cases where contingency plans involves cross-border contingency measures.

Further information on the responsibilities of NSAs with regard to contingency is provided in Appendix J - Contingency Planning Frequently Asked Question (FAQs) (Questions 2 to 7).

5.4 ROLE OF ANSPS

I) POLICY

The ANSPs' first responsibility is the development of the contingency plan, the definition of the measures and alternative services needed in case of degradation or interruption of their services, and their inclusion into a consistent plan, in line with the requirements or targets set by the State.

The preparation phase includes the definition of the measures and the coordination with other actors, i.e. the State, the NSA(s), possibly the other ANSPs, the insurance companies (refer § 5.5.2 Insurance.) The ANSP is in particular responsible for developing the list of addressees to be notified in case an outage occurs and the service is discontinued. It should also, in coordination with the regulator, fix the minimal set of information and time of delivery to be delivered to neighbouring ACCs or States.

The ANSP is also responsible for the implementation of the plan in appropriate cases.

II) PLAN

Coordination with other ANSPs

When the contingency measures envisaged have an impact or depend on other service providers, the ANSP needs to ensure the adequate cooperation with them.

In States where European legislation applies, and where the nature of the contingency measures is such that it requires the use of other ANSPs services or facilities, the ANSP needs to comply with Articles 10.1 and 10.2 of Regulation No 550/2004 which provides:

> *"Air navigation service providers may avail themselves of the services of other service providers that have been certified in the Community.*
>
> *"Air navigation service providers shall formalise their working relationship by means of written agreements or equivalent legal arrangements, setting out the specific duties and functions assumed by each provider…"*

Contingency can be the subject of an ad-hoc agreement or part of a more generic arrangement between the ANSPs.

In principle, an ANSP may sub-contract the provision of services to a third service provider provided that this sub-contractor is certified, that the delegating ANSP (and the States concerned) formally approves the sub-contract, that this arrangements is supported by written agreements properly reflecting the allocation of liabilities.

It would be useful for the ANSP to address, where possible, contingency aspects in its relations with external providers and suppliers. The adequate safety verification of these services foreseen in Regulation (EC) No 2096/2005, Annex II, § 3.1.2, can be best secured through contractual commitments and obligations, which could address where possible, contingency aspects.

Coordination with the NSA

Necessary relations will take place between the ANSP and the NSA in the course of the verification foreseen in paragraph 8.2 of Annex I to Regulation No 2096/2005.

In addition, the ANSP has to formally notify the NSA of its arrangements with other ANSPs.

Coordination with the State

As stated above, the State has the responsibility to make its requirements in the contingency domain known and binding on the ANSP.

As required by both the Chicago Convention and the SES legislation (in particular Article 10.3 of Regulation No 550/2004) the ATSP needs to communicate the intended plan to the State and obtain its approval, when the plan includes the use of other ATSPs' services.

This approval can take several forms, depending on national circumstances and legislation: the approval can be given in advance, subject to communication of the subsequent plans; the approval can be expressed by the joint signature of the contingency plans or by a separate unilateral act by the State (e.g. letter of approval). The (State) approval of the content of the plan can also be delegated to the NSA.

In many States, ATS at airports are provided by other than the national administration or the National ATS Provider. In strategic ATS contingency planning, it is often the National ATS Provider who will need to provide planning which assures that ATS continue to be provided at airports regardless of who normally provides this service at a specific airport.

III) ACHIEVEMENT

The following actions/elements are part of the role of the ANSP:

- Development and testing of contingency plans;
- Coordination with other ANSPs and conclusion of appropriate agreements; communication of these agreements to the NSA;
- Inclusion of appropriate provisions in contracts with other suppliers;
- Inclusion of the contingency plan in the ANSP's insurance coverage;
- Obtain the approval of the NSA, in accordance with requirements of Regulation No 2096/2005, and with requirements set by the State;
- Obtain the State's approval for agreements between ATSPs;
- Implement the Plan where necessary.

5.5 LEGAL ASPECTS

Main legal issues take place when two different legal entities (i.e. two different States, two different ANSPs, civil and military ANSP) collaborate in contingency situations (contractual liability), or when execution of contingency measures has an impact on third parties (third party liability).

5.5.1 LIABILITIES

I) POLICY

In application of Article 28 of the Chicago Convention, States are responsible for the (safe) provision of air navigation facilities and services in their airspace. Any failure to exercise fully and correctly this responsibility may incur the liability of the State.

In a context where the service providers are separated from the State regulator, the responsibility and associated potential liabilities are also dissociated:

- ANSPs, like every legal person, are responsible for their acts or negligence (or those of their staff) and can be held liable for the damage they cause to third parties.
- The State can be held liable for lack of proper oversight; considering the text of the Chicago Convention, it could be argued that the State could also be held directly liable for the non-availability of the services, the inadequacy of the contingency plan or the failure to apply it.

Liability vis-à-vis third parties has to be distinguished from the contractual liabilities between the concerned parties in a service provision environment. The third parties' liability regime (i.e. actions by plaintiffs) is governed by national laws and sometimes public or private international law.

The allocation of liability between the cooperating parties, as well as possible recourse actions, place of jurisdiction, dispute settlement procedures between the players (e.g. States, NSAs, and ANSPs) can be organised through agreements, contracts or regulatory acts. This is of particular importance in the context of contingency plans involving several ANSPs and/or cross-border cooperation (See 5.6 Cross-border Provision of Services and Sovereignty Issues below). However, if written agreements can arrange the liability between the parties, they cannot arrange the right of actions of potential victims.

Delegations of services or arrangements between ANSPs do not lift/remove the responsibilities and potential liabilities of

[7] An indicative checklist of the elements to insert in a Contingency Agreement between ANSPs is provided at Appendix F.

[8] See also Appendix J, Question 13.

the delegating ANSP (e.g. failing ANSP), which remains the one originally designated by the State in which airspace the service is provided.

The liability of the ATCOs involved in an accident when working under degraded or contingency modes would remain, but the level of the due diligence exercised would probably be assessed against the particular context and help mitigating the liability exposure .

As a last remark, it should be outlined that the type of damage for which the liability of players can be invoked depends also from applicable national laws. National laws would help determine for instance whether economic damage suffered by airlines after the closing or restriction of airspace could be the subject of a claim.

II) PLAN

All players involved in contingency planning should know the extent of their potential liability, and where possible clarify and allocate them in writing.

III) ACHIEVEMENT

States should, when they set requirements for contingency, also foresee the possible negative consequences of the failure by the ANSP to meet these requirements (for instance in designation act, in law or regulation, etc…) and verify that the appropriate legal instrument includes provisions to that effect. If the States conclude agreements between them related to contingency, these agreements should contain provisions on the allocation of liabilities. The same applies to the agreement between NSAs.

ANSPs when concluding contracts with suppliers or contingency agreements with other ANSPs should include provisions on allocation of liabilities between themselves vis-à-vis action by third parties as well as provisions on actions (or recourse actions) against each other. ANSPs should verify that the agreements contain such provisions.

5.5.2 INSURANCE

I) POLICY

In application of SES legislation, in particular § 7 of Annex I to Regulation (EC) No 2096/2005, ANSPs are in principle covered against the risks resulting from their operations, mostly via insurance policies or State guarantees. This coverage should extend to the execution of contingency measures by the ANSP as an aiding unit, and also if possible to support provided by other ANSPs to the ANSP as a failing unit.

II) PLAN

The coverage by insurers (or the State if there is a State guarantee) should be secured in case the contingency plans are implemented.

III) ACHIEVEMENT

Contingency plans developed by the ANSP should be communicated to their insurers once they have been approved by the parties concerned.

5.6 CROSS-BORDER PROVISION OF SERVICES AND SOVEREIGNTY ISSUES

The cross-border provision of services raises three issues:

1. The necessary involvement of the respective States concerned:
   - Policy: in accordance with SES legislation, cooperation between ATS providers (and, where applicable, cooperation involving designated MET providers) requires written agreements subject to State approval. Applied to cross-border cooperation between foreign ATSPs, this principle requires the approval of the two States concerned. For other air navigation services (CNS, AIS) this requirement does not exist in the SES legislation but both in view of the role attributed to States by the Chicago Convention and the potential impact on domestic ANS, it appears preferable that the State of the aiding ANSP be also at least informed (it should be noted that all ANSPs have to notify their NSAs of their agreements).
   - Plan: The approval of the State of the aiding unit and of the State of the failing Unit needs to be secured.
   - Achievement: Two schools of thoughts can be proposed: either the States arrange these issues between themselves and respectively delegate the detailed development of the plans to their ANSPs, or the ANSPs conclude a contingency plan/agreement between themselves that is submitted by each of them to their respective State for approval.

2. The cooperation between the NSAs
   - Policy: in application of Article 2.4 of Regulation (EC) No 550/2004, NSAs shall make appropriate arrangements for close cooperation with each other to ensure adequate supervision of ANSPs certified in one State and providing services in airspace falling under the responsibility of another State. This extends to the situations where an ANSP is an aiding or failing Unit in cross-border contingency plans.
   - Plan: the two (or more) NSAs concerned should cooperate, in the verifi-

cation of the compliance of contingency plans

- **Achievement:** each NSA remains responsible for the continued supervision of the ANSPs it certified. As a consequence, the NSA verifying the compliance of the contingency of an ANSP involving a foreign ANSP as an aiding Unit needs to take the initiative to seek information on the aiding ANSP. The cooperation with the foreign NSA will be organised through procedures and processes formalised, if necessary, in written agreements.

3. Applicable rules and regulations:
   - **Policy and Plan:** in the absence of prescriptions to this effect in the international or European legislation, it is left to the discretion of the parties involved to determine which rules and regulations (such as operational procedures) have to be applied should an aiding Unit have to provide services in a foreign airspace. The parties might prefer to decide on the application of the rules of the State in the airspace of which the services are provided. They might also decide otherwise, considering the difficulty in training staff to apply foreign rules.
   - **Achievement:** This matter should be clarified as part of the contingency, be approved by the respective States and be included in the relevant agreements (between States, or between ANSPs as approved by States).

In principle, the State in which the occurrence happened is responsible for incident/accident investigation. Other States may participate to the investigation. It is recommended that States (or ANSPs with the formal approval of the States) cover this aspect in their agreements.

In the absence of prior agreement between them, States do not owe each other a duty of care, in application of the sovereignty principle and because the responsibility of a State is limited to its own territory .

5.7 CONTINGENCY IN MULTI-STATE OPERATIONS

Paragraph 5.4 of Attachment C to Annex 11 to the Chicago Convention recommends that in the case of multi-State ventures, detailed coordination leading to formal agreement of the contingency plan should be undertaken with each State. Similar coordination should also be undertaken with those States whose services will be significantly affected, and with international organisations concerned.

Article 5.4 of Regulation (EC) No 551/2004 provides that a functional airspace block (FAB) shall only be established by mutual agreement between all Member States. The EC legislation does not contain any explicit provisions on the specific case of contingency in FABs.

In both cases, a written agreement between the States concerned shall, therefore, pre-exist and contain provisions on contingency. The States will likely include a high-level requirement for a contingency plan in such Agreement and allocate the development of the plan to NSAs or other State authorities. This later two-level approach is the most likely to be applied.

The EUROCONTROL FAB Model Agreement of 2007 suggests the following provision: *"The Contracting States shall ensure that the ANSPs develop a common Contingency Plan for all the services provided within the FAB establishing the procedures among the Units/Authorities concerned. The Plan shall be developed in compliance with, inter alia, the requirements of Annex 11 to the Chicago Convention. The Contingency Plan shall be developed before the start of the operations of the FAB".*

It would be useful that the States - or their NSA(s) - also agree on the mechanisms for coordination between them, for instance with regard to the common definition of requirements, the joint oversight by the FAB NSA(s) and the approval of the contingency plans.

Furthermore, as recommended by Annex 11 to the Chicago Convention, the States may have to ensure formal coordination with those neighbouring States which might be significantly affected in case of contingency.

Any contingency plan developed by the ANSPs operating in the FAB will have to be a joint/coordinated plan, also agreed upon through a written agreement, and will need to be prepared before the start of operations of the FAB.

The principles relating for instance to the applicable operational rules, the respective liabilities, etc. will be determined by the parties and included in the respective agreements (see preceding Section on cross-border provision of services for more details).

In conclusion, all ANSPs providing services in the airspace constituting the FAB (that airspace will necessarily be defined in the FAB Agreement) should establish a joint contingency plan, or at least coordinate their respective plans. Approval of the contingency is a prerequisite to the FAB.

[9] On cross-border aspects, see also Appendix J (Questions 10 to 17).

The relations with regard to contingency between ANSPs part of a FAB and other ANSPs operating outside of the geographical limits of this FAB (whether laterally or vertically -e.g. in airports) should be treated mutatis mutandis in the same way as cross-border provision of services.

CHAPTER 6. ORGANISATIONAL ASPECTS OF CONTINGENCY PLANNING

This part of the Guidelines provides more specific advice on the organisational issues that need to be confronted at various working levels within ANSPs to construct and then implement contingency plans. It identifies the individuals or personnel and groups involved in contingency planning and contingency execution phases (these may or may not be the same personnel).

In an ANSP, for a given ANS unit (e.g. ACC, APP, and TWR), the organisational aspects may be addressed and processed as follows:

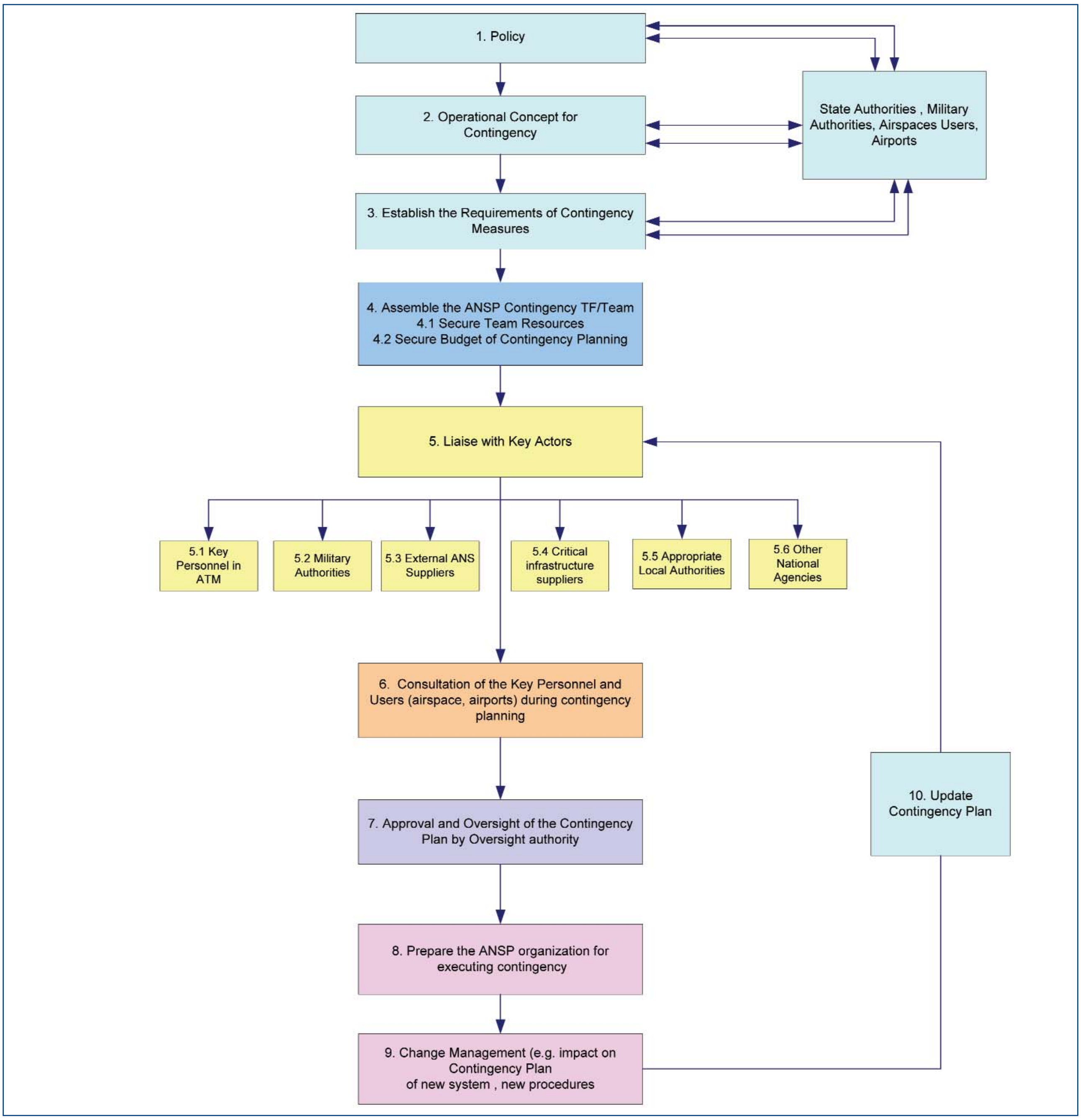

1. Policy
2. Operational Concept for Contingency
State Authorities , Military Authorities, Airspaces Users, Airports
3. Establish the Requirements of Contingency Measures
4. Assemble the ANSP Contingency TF/Team
4.1 Secure Team Resources
4.2 Secure Budget of Contingency Planning
5. Liaise with Key Actors
5.1 Key Personnel in ATM
5.2 Military Authorities
5.3 External ANS Suppliers
5.4 Critical infrastructure suppliers
5.5 Appropriate Local Authorities
5.6 Other National Agencies
6. Consultation of the Key Personnel and Users (airspace, airports) during contingency planning
7. Approval and Oversight of the Contingency Plan by Oversight authority
8. Prepare the ANSP organization for executing contingency
9. Change Management (e.g. impact on Contingency Plan of new system , new procedures
10. Update Contingency Plan

Figure 4: Contingency Organisational Aspects Process

The explanatory notes that follow are numbered according to the related in figure4.

NOTE 1: POLICY

The requirements for Contingency measures are founded in the ANSP's Policy (see 7.1 Policy). This policy will in part be determined by national (State) requirements and on ANSPs' overall corporate objectives.

NOTE 2: OPERATIONAL CONCEPT FOR CONTINGENCY

The broad Policy objectives should be transformed into an Operational Concept for Contingency (see 7.3 Operational Concept). This Concept will demand that a set of requirements is agreed between all relevant stakeholders to realise the Concept and therefore satisfy the Policy objectives.

NOTE 3: ESTABLISH THE REQUIREMENTS OF "CONTINGENCY MEASURES"

The requirements setting process is iterative and cyclical by nature and will involve consultation between State authorities (including the Military authorities), the Air Navigation Services Providers (ANSPs) and the Users (Airspace Users and Airports) as detailed in Chapter 7.

NOTE 4: ASSEMBLE THE ANSP CONTINGENCY PLANNING TEAM

Constructing and writing contingency plans is not a one man job, but the job of the management and the staff of an ANS provider. Contingency planning involves practically every aspect of running an ANS Unit, It requires specialists from service provider management, air traffic controllers, technical and engineering personnel and other ATM services personnel including safety and ATM security specialists, legal department, human factors, human resources and if appropriate staff representatives. . The involvement of front-line practitioners such as ATCOs and ATSEPs has been found to be especially helpful in identifying contingency solutions that are practical and workable. A starting point could be to organise a meeting, workshop or a brainstorming session of the Contingency Planning Team. The purpose would be to review any existing material (Policy, Operational Concept, Contingency Plans) to gain a deeper understanding of what is required to undertake the contingency planning effort.

Contingency Planning groups may be formed not only to develop the contingency plans but also to assist with their implementation and execution if ever there is a need.

The process of building contingency plans should be owned by managers at the appropriate level (e.g. directors). The owners should be responsible for ensuring their individual plans are current and that information contained in the plans remains valid. The owners should be clearly identified in the contingency plans. It is normal practice for a senior manager (e.g. Senior Operations Director) to sign-off the contingency plan(s).

Those responsible for maintaining the document should also be identified. Resources and budget of the contingency planning team activities should be secured.The resources and budget for the actual contingency measures should be appropriately addressed during the corporate planning process and secured within the organisation as necessary.

NOTE 5: LIAISE WITH KEY PERSONNEL DURING THE WHOLE PROCESS

Note 5.1: Key Personnel in the ATM

a) National experts and Users

Depending on the nature of the outage being considered or on the geographic location of the ANSP unit (e.g. ACC, APP, TWR ..) in question, there is likely to be a need for national coordination between experts (e.g. State authorities, other ANSPs, Airports and Airspace Users) to deal with strategies in respect of outages whose effects can be localised, and thereby only require national planning.

b) International experts (if relevant)

Operational experience has shown, backed up by simulations conducted by EUROCONTROL during 2008, that the effects of even seemingly insignificant events cannot always be contained within national borders. Indeed, the effects of contingency are usually widespread and where this is the case , then external coordination involving the EUROCONTROL Central Flow Management Unit (CFMU - see below) and experts from adjacent states is likely to be appropriate if it is necessary to address the implications on adjacent ATS Units which may, for instance, be located in another State.

c) Coordination with CFMU and OCG

ANSP contingency plans have, by nature, an impact on the European ATM Network. Therefore such planning for crisis and disaster should be made with CFMU involvement, in order to organise the process and alleviate the impact on the Network. The management of these activities should be owned by the Operational Coordination Group (OCG).

All Network actors should be kept informed of contingency developments therefore, it is essential to include the CFMU during all phases of contingency and contingency planning:

- Normal Contingency Planning
- Before a known crisis/contingency
- During crisis/contingency
- During the recovery phase after crisis/contingency

More detailed considerations concerning the input of the CFMU in the contingency planning process are at Chapter 11 Execution and Assurance.

d) High Level Tactical Management - Crisis Management Group

A crisis management structure, the Crisis Management Group (CMG) has been created which aims to react quickly and efficiently when unexpected situations seriously disturb air traffic flows in ECAC airspace. This group is chaired by the Director of the CFMU and is composed of nominated representatives of the Directors of Air Navigation.

The objectives of the CMG are, inter alia, to support possible arrangements worked out by the CFMU, in conjunction with national experts, regarding:

- The removal of the cause of the crisis or, if that is not possible;
- the increase in ATC capacity to alleviate the effects of the crisis;
- the assurance that the arrangements made by the experts and agreed by the CMG are supported by their administrations and are implemented;
- the assurance that priority rules established for use in the crisis are applied and implemented.

In view of the mandate and aims of the CMG, States are recommended to include in their contingency plans, an action to co-ordinate with the Director CFMU and convene the CMG, if appropriate. According to the situation, the CFMU will consult with Directors of Operations of the ANSPs and decide if a CMG is required.

e) Coordination with ICAO

The effect of service disruption upon international air traffic flows and on the provision of ATS in adjacent airspace can, depending on duration and circumstances, be significant. In those cases there is a requirement for international/(sub) regional initiatives and co-ordination, involving as necessary other States, ICAO, the CFMU and Airspace Users (Chapter 2.30 of Annex 11 to the Chicago Convention). Contingency plans should therefore be prepared, tested and promulgated before the occurrence of events, in consultation with other States and ICAO, as appropriate, preferably at (sub) regional level. For more information, refer to 9.1.4 Airspace including ICAO Aspects

Note 5.2: Liaise with the Military authorities

Military authorities are major participants in ATM and their role can be even more prominent in the context of contingency. In particular, the military have key roles to play in ATM Security matters as described in 10.3 Security (Collaborative Support and Self-Protection).

Note 5.3: Liaise with External Air Navigation Services suppliers

In the context of EUROCONTROL Safety Regulatory Requirement 3 (ESARR 3) "*the ATM service-provider shall ensure adequate and satisfactory justification of the safety of the externally provided services, having regard to their safety significance within the provision of the ATM service*". Therefore, in case an ANSP avails itself of services of other ANSPs, it should consider the possible causes of loss/disruption of services related to a failure in the delivery of external services and these suppliers should be consulted, as relevant, when developing the contingency plans. More advice on external suppliers can be found in Appendix G.

Note 5.4: Liaise with Critical Infrastructure suppliers

An ANSP should pay particular attention to the possible causes of loss/disruption of services related to failure(s) of critical infrastructure such as network suppliers, e.g. IT, communications or power supply. In addition, in certain countries (e.g. the UK and the US) specialist planning groups of experts support the resilience of national computational infrastructures. Those organisations are better prepared than ANSPs to conduct the political/security threat assessments.

Note 5.5: Liaise with appropriate local authorities

Similarly, an ANSP should liaise with the local authorities within whose area the ANS unit is located. The appropriate local authorities would have a major role to play in case of catastrophic outages such as natural disasters (e.g. flood, fire), chemical "SEVESO" type accidents, security incidents such as terrorist acts, and pandemics. They would keep the roads open (access to the ANSP premises), liaise with the police etc. ANSPs and local authorities should be mutually aware of each other's contingency plans.

Note 5.6: Liaise with other national agencies

ANSPs also need to liaise, possibly via the Regulator/NSA, with national contingency planning agencies whose activity is dedicated to specific events. For instance, in the context of Security, it might be necessary for local ANSP task forces to request external input from these other wider organizations already engaged in contingency planning in this area (e.g. National Counter Terrorism Security Office - NaCTSO- in the UK).

NOTE 6: CONSULTATION OF THE KEY PERSONNEL AND USERS DURING PLANNING AND CONTINGENCY OPERATIONS

All the organisations previously listed as "key personnel" should be consulted during the Planning stage to ensure a consistent and consolidated approach of contingency. They may be involved in the actual contingency operations as necessary. In particular, due to the critical role of the CFMU, its role is further detailed in Chapter 11 (Respective roles of the ANSPs and CFMU).

In addition, consultations with Airspace Users and Airports (if relevant) are essential both during the Planning phase and during the Contingency itself. In the Planning phase, it is important that Airspace Users provide inputs into potential solutions. During the Contingency, it is essential that Users are regularly provided information on the status of ATS as up to date as possible. This may consist of, inter alia, briefings to operators by electronic means on a regular basis (e.g. NOTAMs).

NOTE 7: APPROVAL AND OVERSIGHT OF THE CONTINGENCY PLAN(S)

In the States where European legislation applies, the NSA should undertake the initial oversight investigations of the contingency plan(s). It is advisable to involve the NSA early enough to ensure a common understanding of the obligations and facilitate approval of the Contingency plan (e.g. in the context of certification of ANSPs). Ultimately the plan should be submitted to the NSA for formal endorsement.

The contingency plan(s) would be reviewed periodically on a frequency (in terms of years) to be decided by the NSA. However, the ANSP should be prepared for any on-spot audit of the contingency plan(s) that the NSA may deem necessary.

NOTE 8: PREPARE THE ANSP ORGANISATION FOR EXECUTION OF CONTINGENCY

One key to a successful contingency plan is the early identification of clearly defined roles, responsibilities and authorities (see Chapter 5). This would allow ANSPs to manage contingency programmes and processes throughout the organisation and ensure the continued readiness of the appropriate personnel to respond when required. The personnel involved in the contingency execution phases may or may not be the personnel involved in the contingency planning and consultation.

By assigning roles and responsibilities, ANSPs can ensure that the tasks required to implement, execute and to maintain the contingency plan can be monitored. It is recommended that a member of the ANSP Executive e.g. the Operations Manager/ Director of operation should be given overall accountability for the implementation and execution of the service unit's contingency plan(s).

NOTE 9: CHANGE MANAGEMENT

Contingency plans should be resilient to change. A mechanism should be established to check relevant contingency plans after all changes (e.g. system changes, procedures changes, organisation changes, environment - change of power supply provider -).

NOTE 10: UPDATE CONTINGENCY PLANS

Contingency Plans should be updated following the outcome of change management.

CHAPTER 7. POLICY, OPERATIONAL CONCEPT AND SETTING REQUIREMENTS

7.1 POLICY

It is recommended that ANSPs develop a policy for Contingency Planning in much the same way as they do for Safety and Security. Moreover, the Policy should be coordinated with the organisation's overall approach to Crisis Management - see Chapter 13.

The Contingency Policy should set out the organisation's attitude towards Contingency and state the overall Contingency goals and objectives. It should be explicit about the scope of Contingency within the organisation, e.g. whether it wishes to include the provision of Service Continuity or limit provision to 'fail to safe' modes of operation .

The Contingency Policy sets the internal requirements for Contingency and provides a framework to enable the development of an Operational Concept for Contingency. Furthermore, the Policy should outline the principles that will underpin the detailed contingency planning actions and measures that will be developed later in the Planning process.

In addition, the Policy should broadly reflect:

- The performance criteria to be satisfied, e.g. service levels, capacity, environment, efficiency and reaction time.
- The units covered: is it all or only some?
- The Contingency Planning testing/exercising regime.
- The assumptions and limitations related to ANSP Contingency Planning
- The guiding principles relating to safety, security, continuity of service provision (or not) and adaptability.
- Senior management commitment to contingency, specifically the need for management to:
    - Create and maintain awareness of the importance of fulfilling the principles of Contingency Policy.
    - Develop, implement and maintain Contingency Plan(s).
    - Develop and establish resilience by investing in redundancy.
    - Assure the economic stability of the company by implementing Contingency Policy.
- Relationships with internal parties (Engineering/technical, safety, security etc).
- Relationships with external parties such as surrounding ANSPs, airports, NSAs etc.
- The needs expressed by airspace users, regulators, service providers and any other stakeholders that might be affected by ANS contingency.
    - Each party involved should know and understand which set of requirements are to be further defined in their own organisation to contribute to a safe and efficient deployment of contingency measures.
- Considerations of key risks that the organisation has identified and that it wishes to be protected against.

7.2 VALUE OF CONTINGENCY

The added value of Contingency Planning to ATM and how it underpins the ATM service and business needs could also be described. The value of Contingency when applied effectively:

- Supports service and business risk management.
- Assures employees.
- Assures customers.
- Builds confidence.
- Helps to protect and enhance reputation.
- Meets legal and regulatory requirements.
- Makes sound business sense.
- Influences insurance premiums.
- Protects people and assets.
- Contributes to safeguarding Critical National Infrastructure.
- Aligns with safety and security policies.
- Supports national and international ATM networks.

7.3 OPERATIONAL CONCEPT

7.3.1 RATIONALE FOR DEVELOPING OPERATIONAL CONCEPT FOR CONTINGENCY (SERVICE CONTINUITY)

An Operational Concept for Contingency should provide the following benefits:

- A common language between all parties involved, i.e. State(s), ANSPs, Military organisation(s), Airspace users, Airports, etc…, to capture needs, set-up requirements that avoid misunderstandings.
- A set of clearly defined requirements that will further support the definition and implementation processes.
- A set of safety, security and performance criteria to be satisfied by the

[10] Economic guidelines presented in Appendix H may assist ANSPs and NSAs to form an opinion as to limiting provision to "fail & safe" modes of operations.

future system.

- Consistency with recognised safety assessment techniques such as the EUROCONTROL SAM and the Safety Case Development methodologies that start their assessment process from the OPS concept downward to the system design approach. *(Note: In the same way the Operational Concept also needs to be consistent with the aims and objectives of the ATM Security Risk Assessment Methodology to ensure that specific ATM Security threats are properly captured.).*
- An Operational Concept also helps to provide a setting to undertake the economic assessment of Contingency - see Appendix H.

7.3.2 DESCRIPTION OF AN OPERATIONAL CONCEPT FOR CONTINGENCY

An Operational Concept for Contingency could contain all or some of the following elements:

- Purpose and use (refer chapter 7.3.2.1)
- Policy inputs
  - Contingency Principles (safety, security, continuity)
  - Contingency Criteria
  - Contingency Key Events (i.e. foreseen contingency situations) and related Risks
- Legal requirements
- Candidate Contingency strategies ;
  - Preferred option(s) - the chosen Contingency Planning strategy
- Consultation Process
- Economic Aspects
- Current Contingency Arrangements
- Description of the New Environment
- Description of Changes
- Summary of Impacts and Analysis of Changes

Each of these steps is described in later sections of this Chapter. In addition the Operational Concept should also refer to and include:

- Responsibilities- personnel and actions
  - Decision making (Management or Supervisor)
- Contingency planning process/ steps (see 8.2 Planning Process);
- Reference documents
- Definitions and acronyms- terminology

7.3.2.1 PURPOSE AND USE

The development of an Operational Concept for Contingency situations begins with the elaboration of the Contingency Policy and moves the planning process away from the high level of abstraction of the Contingency Life Cycle.

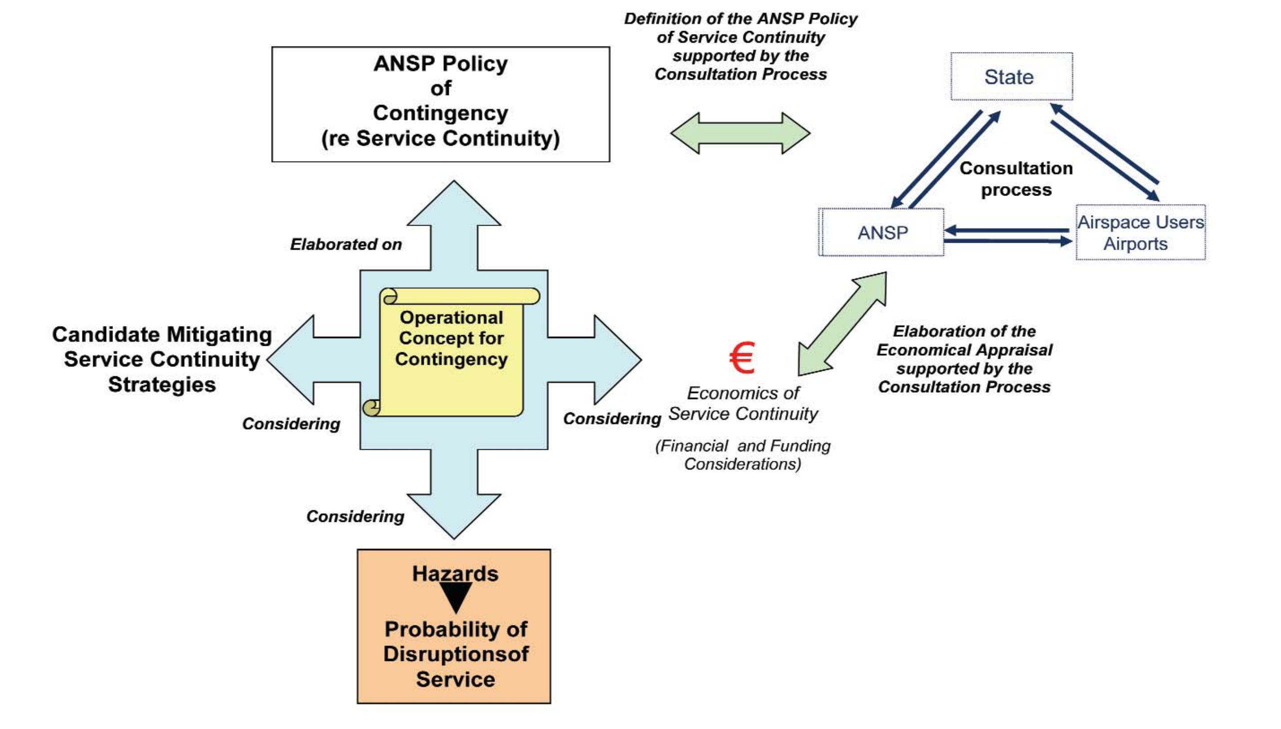

Definition of the ANSP Policy of Service Continuity supported by the Consultation Process
ANSP Policy of Contingency (re Service Continuity)
State
Consultation process
ANSP
Airspace Users Airports
Elaborated on
Operational Concept for Contingency
Candidate Mitigating Service Continuity Strategies
Considering
Considering
Considering
€
Economics of Service Continuity
(Financial and Funding Considerations)
Elaboration of the Economical Appraisal supported by the Consultation Process
Hazards
Probability of Disruptionsof Service

Figure 5: Process supporting the definition of the Operational Concept for Contingency

7.3.2.2 POLICY INPUT

As for all concept documents, it is critical to clearly delineate the scope of the contingency concept including its context, assumptions and limitations as far as they exist. Reflecting the high level contingency planning objectives included in an ANSP's Policy or Statement of Intent on Contingency, and aligned with corporate Crisis Management policies and plans, there should be a description, for example, about whether the concept addresses an entire National ATM system, only a part of it or if it is developed in a bi-lateral or multi-national context, e.g. FAB. Assumptions should cover aspects that are a-priori excluded from the scope of the concept for given reasons or aspects that might be taken into consideration according to specific justifications. Limitations are composed of all aspects for which the concept cannot define contingency solutions/measures in line with the expected criteria.

Guiding Principles

Guiding principles to be followed in defining and implementing contingency concepts should, inter-alia, address the following:

- ***Safety:*** The target level of safety for contingency measures should be the same as for Normal Operation.
- ***Security:*** The reference level of Security should be the level when working under Normal operations.
- ***Continuity:*** Service Continuity is a dimensioning factor (depending on the Policy) when designing contingency measures to ensure a minimum level of service to be provided (capacity criteria).
- ***Adaptability:*** The contingency measures should be designed in such a way that they can easily adapt to a different mix of events or situations.

Criteria

It is the role of the Operational Concept to define criteria to be satisfied when the systems are implemented and activities performed in order to fulfill its requirements.

Provided that "by principle" the safety and security levels should not be compromised under Emergency, Degraded modes of operations, Service Continuity or any other abnormal situations, the remaining criteria to be looked after for contingency are (not exhaustive):

- Capacity: adjustable according to the contingency phase.
- Environment: controls/constraints may be relaxed to permit contingency ops.
- Efficiency: have the ability to re-coup losses as quickly as possible to maintain commercial viability.
- Reaction time: time required to implement measures.
- Recovery steps: how much of an ANSP's capabilities will be restored and by when.

Key Contingency Events and related Risks

The Contingency Policy or Statement of Intent should include a list of the key contingency events and related risk areas that the organisation has identified and that it wishes to protect itself against. These could include:

- Potentially frequent situations (e.g. partial loss of radar coverage, unavailability of ODS) where disruptions would partially affect ANSPs during short periods of time (ranging from some hours to a few days) to
- Infrequent situations (e.g. major software bug, floods, earthquakes, terrorist attacks, pandemics, where complete ATM Units could be totally out of service for long periods of time.

7.3.2.3 CANDIDATE CONTINGENCY STRATEGIES

A variety of ANS contingency strategies are available to help ANSPs move away from the high level abstraction of the Contingency Life Cycle and to begin the elaboration of the Operational Concept towards more detailed planning of contingency measures. The Operational Concept in defining the scope, context and criteria of contingency solutions/measures should indicate what strategies are to be further detailed within the contingency plan(s). Brief descriptions of some strategies are shown below; they are described in detail in Appendix C.

Co-Located Facilities (National): Some 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 events could eliminate both primary and contingency resources. Military facilities may also be considered.

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.

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.

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.

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, whilst such arrangements show that it is theoretically possible to use them for contingency provision, the reality on the ground suggests that the actual practical implementation is fraught with difficulties. For instance, such agreements require 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. Moreover, it can be difficult to coordinate the drills that are required to ensure that these agreements can be implemented. Licensing and regulatory issues associated with provision of services in another State's airspace need to subject to binding state agreements.

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.

It is stressed that the strategies listed above are not mutually exclusive and it may be necessary to use several different approaches or combinations of approaches to meet ANSPs' needs. The approach adopted by particular stakeholders will often be determined by local constraints. ***One critical element that should not be under estimated is the role of engineering and technical support in devising and implementing contingency*** (refer Chapter 9 ANS Related Planning Considerations and Appendix G - Systems Engineering Perspective on Contingency Strategies).

7.3.2.4 CONSULTATION PROCESS

The Operational Concept should capture all the needs expressed by airspace users, regulators, service providers, airports and other stakeholders that could be affected by an adverse event. A detailed exposition of the Consultation Process is given later in this Chapter.

7.3.2.5 ECONOMIC ASPECTS

Financial and funding considerations will also have to be included in the Operational Concept. They are briefly described at Section 7.5 Financial Dimension of Contingency and more fully in Appendix H - Principles for the Contingency Plan Economic Assessment.

7.3.2.6 CURRENT CONTINGENCY ARRANGEMENTS

It is paramount to describe, as precisely and realistically as possible, the current situation in terms of modes of operations, environment and resources involved. From this description a gap analysis can identify the requirements necessary to achieve the set up objectives.

The description should include (indicative):

- A functional description of the current system.
- Different modes of operations and associated implementation procedures.
- Built-in resilience and redundancy features.
- Interfaces to the external world.
- Involved personnel, i.e. skills/competences, responsibilities, organizational structure, etc…
- Performance criteria.

- Quality, safety and security standards applied.

7.3.2.7 DESCRIPTION OF THE NEW ENVIRONMENT

The outcome of the previous steps should enable the description of the new environment in which it is foreseen the Operational Concept will be set. Contingency Plans will not derogate to the rule and prior to conducting contingency systems/measures safety assessments, safety case developers should try to demonstrate that the contingency concept as a whole is intrinsically safe (SCDM "Safety Case Development Manual", Edition 2.0, Sept2005). The selected scenarios should encompass all changes that are required to achieve the concept requirements.

7.3.2.8 DESCRIPTION OF CHANGES

The description of changes should include:

- Justification for changes based upon the selected scenarios, i.e. user needs, missions, environments, interfaces, personnel or other factors that require a new or modified system, deficiencies or limitations in the current system or situation that make it unable to respond to these factors.
- Description of the new/changed system, this part should, as far as practicable, follow the same structure as the "current contingency arrangements" in order to better identify the differences and conduct an easier assessment of the changes.
- Affected personnel, i.e. skills/competences, responsibilities, organizational structure, etc…
- External support required to conduct the changes.

7.3.2.9 SUMMARY OF IMPACTS AND ANALYSIS OF CHANGES

7.3.2.9.1 Advantages/Disadvantages of the New Contingency Arrangements

When identifying the Advantages/Disadvantages for the defined changes it is in fact an assessment of scenarios "Pros & Cons" that is conducted. It should be a qualitative and quantitative summary. For example, should the change concern the implementation of a Contingency remote facility, at National or Multi-national level, then all the elements of the ATM system, i.e. Airspace, People, Equipment and Procedures, should be assessed to find out if the impacts of this change on the environment and compared to previous contingency arrangements carry out benefits or disagreements to the overall system.

7.3.2.9.2 List of limitations

All identified limitations should be listed with associated mitigations and/or tradeoffs.

7.4 CONSULTATION PROCESS

The State authorities (including the Military authorities), the Air Navigation Services Providers and the Users (Airspace Users and Airports) should put in place a process to set the policy, operational concept and requirements for "Contingency measures".

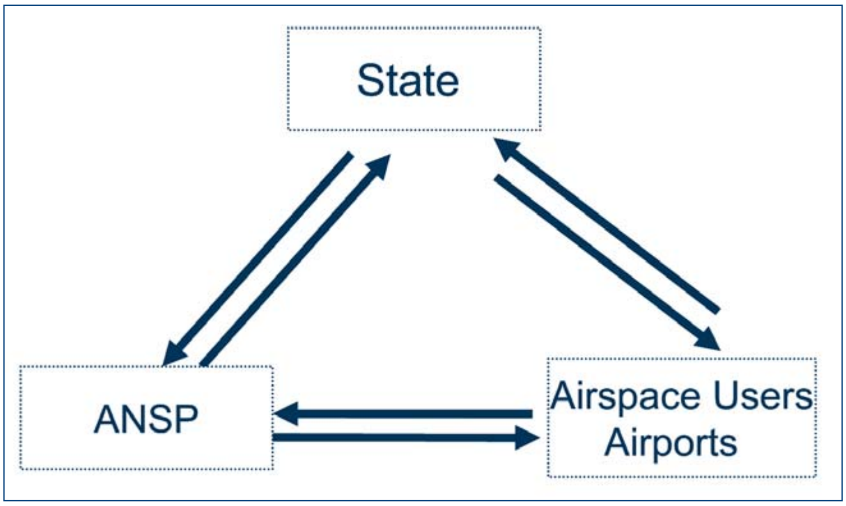


Figure 6: Consultation Process

In this process, the ***State authorities have primacy in defining the requirements.*** ANSPs in consultation with Airspace Users and Airports develop the appropriate measures to meet these requirements and any additional local business objectives stated in their Contingency Planning policy.

7.4.1 STATE / ANSP CONSULTATION

The State authorities (in their rule-maker role) and the ANSPs should establish a dialogue to define the mandatory contingency requirements. The ANSPs will have to fulfil their obligations with regard to contingency planning and by so doing ensure the Safety related elements of providing ANS and associated services, whilst also meeting, as appropriate, the requirements related to Security, Capacity/Flight Efficiency and Environmental Sustainability. States may also consider other wider political, social and macro economic issues.

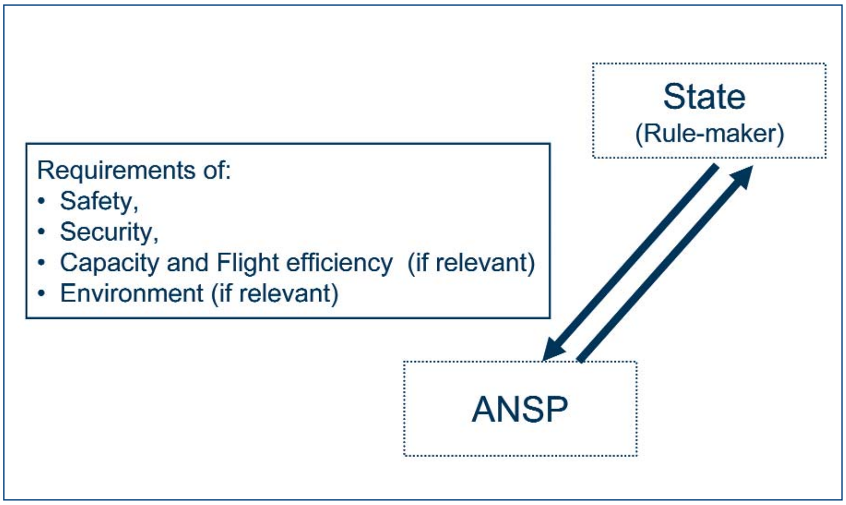

State
(Rule-maker)
Requirements of:
• Safety,
• Security,
• Capacity and Flight efficiency (if relevant)
• Environment (if relevant)
ANSP

Figure 7: State/ANSP Consultation process

The primary considerations between State and ANSP will concern Safety and Security. However, according to State decision, capacity requirements (e.g. minimum level of capacity after a certain time) and environmental constraints could be also considered.

7.4.1.1 SAFETY:

The reference is the safety level when working under normal operating conditions. The expectation should be that this safety level should be not be compromised during contingency conditions. In that context, (NSA)/Regulators' approval of the Safety documentation is required.

7.4.1.2 SECURITY:

EC Regulation No 2096/2005 sets requirement on security of facilities, personal and operational data and requires ANSPs to implement a Security Management System (Sec MS). Links should be drawn between the policy making processes that inform both Contingency Planning and Security Management. Moreover, the development of contingency provision should be coordinated with the overall ATM security strategy for the organisation. Alternatively, described in Chapter 7, ANSPs could adopt/implement a distinct Contingency Planning Policy which fully encompasses Security related issues and concerns. The decision on how Contingency Planning and ATM Security are managed is a local (ANSP) decision. Nevertheless it is recommended that at a minimum the following principles should apply:

- Security issues should be considered during planning, procurement, deployment and maintenance of ATM systems including Contingency operations.
- Under degraded modes of operation (contingency) it is necessary to ensure that the loss of key system functionality has not invalidated any of the assumptions that secure normal operations.
- Contingency plans might also consider the additional constraints that particular threats might place upon Service Continuity operations following the loss of an ANS facility. (E.g. terrorist attacks on ATM infrastructures may not only lead to the loss of those infrastructures. They can also introduce additional restrictions similar to those that were put in place in the weeks and months following the attacks on the United States during 2001).
- Security requirements remain valid in Contingency.

The reference level of (ATM security) operations is, therefore, the level when working under normal operating conditions. The Security (airspace, facilities, personnel and data) including unlawful interference with ATM service provision) should not be compromised under contingency conditions. However, it is important to understand that levels of Security are achieved through a mix of measures/controls (Security in depth, layered Security). On this basis an equivalent level of Security can be achieved by applying a different mix/set of measures. Accordingly, the ***same level of Security does not necessarily imply the same controls.*** Contingency planning and measures should be included as a vital element of local Security Management Systems (SecMS).

ATM Security covers 2 major areas:

- ***Self-protection*** of the ATM system against threats aiming at the ATM system and its facilities (including network, personnel and information/data).
- ***Collaborative security support*** to rel-

evant civil and military authorities responsible for countering aviation security incidents, crisis and emergency situations.

The initial objective of Self Protection is the availability and integrity of ATM services resulting in a safe, economic, efficient and orderly flow of air traffic, whereas the objective of Collaborative Support is the availability of support services under the umbrella of airspace security/national defence and/or security requirements.

In that context, the role of State authorities is prominent with a view to defining requirements in terms of minimum Security service levels during ATM contingency modes of operations (e.g. timing and restoration (recovery) of normal operations.). This may also include contingency measures aiming at an early restoration of the service levels making use of alternate (civil and/or military) facilities through relocation of key personnel or the transfer of operations to adjacent units.

Further information on these ATM security related issues can be found at § 10.3.

7.4.1.3 CAPACITY

The ***minimum level of capacity*** to be provided at different time horizons after disruption of services (e.g. 24 hours, 48 hours and longer periods) is subject to policy decisions set by the States and ANSPs.

However, the cost of creating alternate solutions can be prohibitively expensive and the business risks need to be properly evaluated and assessed. In this situation, a 'one-size fits all' solution is most definitely not appropriate or necessary and there will most certainly be a need for ANSPs and users to be fully consulted in the states process for determination of contingency capacity.

7.4.1.4 ENVIRONMENTAL SUSTAINABILITY:

This parameter should be considered in conjunction with flight efficiency, where possible. In this context, contingency operations should be considered against compliance with environmental rules (degree to which environmentally driven traffic rules and constraints imposed on airports and airspace are respected), including atmospheric and noise aspects (e.g. noise generated and its impact on affected population).

7.4.2 ANSP, AIRSPACE USERS AND AIRPORTS CONSULTATION

The primary concern to be discussed between ANSP, Airspace users and Airports should be the capacity and flight efficiency. Environmental issues may also be discussed within this context.

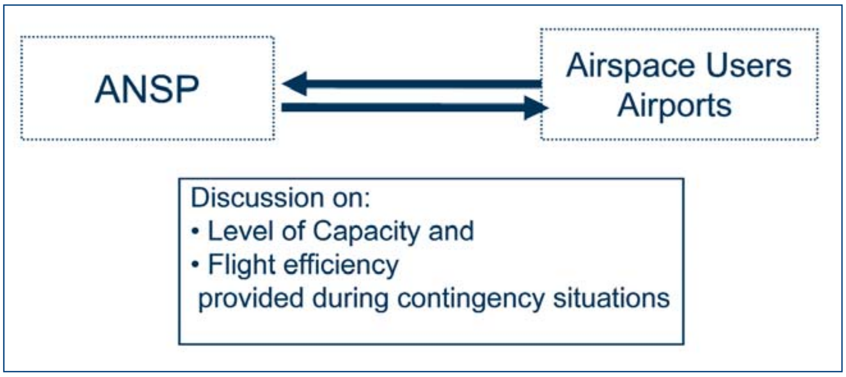


Figure 8: ANSP/Airspace users/Airports Consultation process

The consultation should take place, where appropriate, in the context of the "*formal consultation process with the users of its [ANSPs] services on a regular basis, either individually or collectively, and at least once a year*", in accordance with Regulation (EC) No 2096/2005, Annex I, § 8.1. .

The capacity to be provided at different time horizons after disruption of services (e.g. 24 hours, 48 hours, longer periods) depends on existing alternate solutions (now) and future possibilities (at medium and long term) based on investments (supported by Cost Benefits Analysis) and the available sources of funding.

The flight efficiency parameters should be considered when considering different options. In that context, CFMU plays a major role in coordination with the State/ANSP.

For instance, in the case of an Air Traffic Service provider (ATSP), the Airspace Users should be informed of the different contingency scenarios and their effects on ATSP capacity:

- The consequences of a loss of facility.
- The operational unit(s) that will be utilised for contingency purposes) (aiding units), or the staff who will provide alternate services;
- The level of capacity which will be made available by an ATSP at different time horizons after disruptions (e.g. 2 days, 10 days or 14 days, and later after months (3 months , 12 months)

The Airspace Users should also be consulted on the impact on their operations (e.g. number of aircraft that can be handled by each aircraft operator at the different time horizons after disruptions considered by the ATSP).

In addition to the consultation process stated above, it is recommended that ANSPs consult with the Airport Operators, at those locations where ATS are provided, in order to discuss and obtain agreement, as necessary, on the planned levels of service to be provided in each of the various contingency situations and timings.

7.5 FINANCIAL DIMENSION OF CONTINGENCY

A prime objective in defining contingency plans is to achieve adequate contingency capability at a reasonable cost.

Short-term and long-term investment in contingency will be determined by factors such as:

- The existence of possible alternate contingency locations and systems (inventory);
- The investments and operating costs to reach a given capacity;
- The probability of an accident/failure and any costs or losses incurred as a result of any service disruption/unavailability;
- The potential benefits to have contingency measures implemented (e.g. lower insurance premiums).

Decision-making on investments for Contingency should be supported by Economic Analysis.

It is important to insist that the economic analysis is only a part of the decision making process in Service Continuity. However, no decision to invest depends solely on the results of an economic assessment of candidate strategies. The final decision to invest in Service Continuity should take into account, but not be limited to, other considerations such as:

- Political decision
- Binding nature of the legal framework
- The ability to finance which may vary depending on e.g. the cost of money or the status of the industry at that time
- The need to account for limited financial and/or human resources and priority of the programmes and to spread the required investments over a number of years
- The possibility to link the decision to the outcome of a future technological change
- The opportunity to link the decision to a programmed upgrade of facilities
- The possibility to link the contingency planning for Service Continuity to the success of bilateral or multilateral arrangements, hence to delay the decision as to the strategy until such arrangements are in place
- The attitude of the local airspace users and airports and their willingness to endorse a risk and/or share the burden of the financing of the mitigating strategy
- Conclusions of the safety and security assessment of each mitigating strategy.

High level principles for the Contingency Plan economic appraisal are further developed in Appendix H - Principles for the Contingency Plan Economic Assessment. Methods of economic assessment of contingency plans (e.g. CBA) are addressed at high level. When and how such methods should be used is detailed in the Planning process.

7.6 ANSP "CRISIS MANAGEMENT"

The high-level objective of crisis management actions is to identify potential, impending or actual crises and to respond to these in a co-ordinated and successful manner. Effective crisis management plans should ensure that a measured response is provided to staff, the media and to stakeholders, and where appropriate should ensure service continuity of ANS. Planning for contingency measures should be considered within the larger framework of crisis management. Chapter 13 Crisis Management of the Guidelines gives an outline framework of a possible corporate-level "crisis management plan".

A Corporate crisis management policy should be developed to define guiding principles and set up the policy framework for local crisis management plans. It is recommended that all local crisis management plans should be tested on a yearly basis. The test may range from trialling notification of key personnel to a full-scale practice. Moreover, it is further recommended that all existing and new local crisis management plans should be checked for consistency against the policy and guiding principles contained in the "Corporate Crisis Management Policy" document.

Practices should be as realistic as practicable and initiated with as little warning as possible. However, care must also be taken that everyone understands that what is happening is an exercise which cannot be mistaken for a real-life event.

CHAPTER 8. CONTINGENCY PLANNING PROCESS

8.1 PLANNING GENERAL

The previous sections of the Guidelines set out the Policy requirements for contingency planning within ANS organisations. The aim of this Planning section is to describe a process which ANS organisations may find helpful to identify and develop, as necessary, contingency measures to deal with a broad range of possible contingency scenarios/concepts.

The first part of the process concentrates on the 'Emergency, Degraded Modes and Recovery' modes of the Contingency Life-Cycle whilst the latter looks more closely at the 'Service Continuity' mode. It is important to remember that when it comes to identifying hazards and threats, safety is not the sole consideration and other relevant aspects such as security are taken into account.

The process described attempts to provide a structured, systematic approach and is based around the principles and processes established in the EUROCONTROL Safety Regulatory Requirement 4 (ESARR4) and, for Security related issues, the ATM Security Risk Assessment Methodology (SecRAM). Both of these techniques are based on traditional risk management principles with the aim of improving an organisation's resilience to identified hazards and threats. Indeed, European ATM systems are increasingly designed and operated in accordance with ESARR 4 provisions and this in itself provides levels of ATM system protection through built-in resilience and redundancy features. These would fall in the scope of the 'Normal' operations phase of the contingency life-cycle. Nevertheless, even these barriers can be breached. It is, therefore, logical to extend (in a simplified format) the Safety Assessment Methodology (SAM) embedded in ESARR4 to cover the development and possible execution of ATM contingency measures covering Emergency and Degraded modes of operation and, ultimately, Service Continuity. Moreover, Sec RAM can also be employed to ensure that ATM Security risks are also adequately assessed and managed.

By adopting a SAM/Sec RAM-type approach, ANS organisations should be able to satisfy themselves that any contingency measures that they choose to develop are safe and provide adequate security assurance.

8.2 PLANNING PROCESS

The planning process that follows is presented as a stepped approach. In reality, however, it is an iterative process; some of the activities would run in parallel and it may also be necessary to re-trace some steps as the process progresses

The Planning activities may be organised as follows:

Step 1. Inventory of the Units /services/functions of an ANSP - it is essential that the process to determine contingency strategies be applied to the whole portfolio of ANS units, services and functions (either provided or supplied). It is also necessary to make an Inventory of resources (e.g. systems, assets, procedures, and staff) since this will be the means to identify the additional resources required to satisfy the contingency requirements.

Step 2. Identification of "realistic events" - for each ANS unit, the "events", including security ones, that may lead to loss or dis-

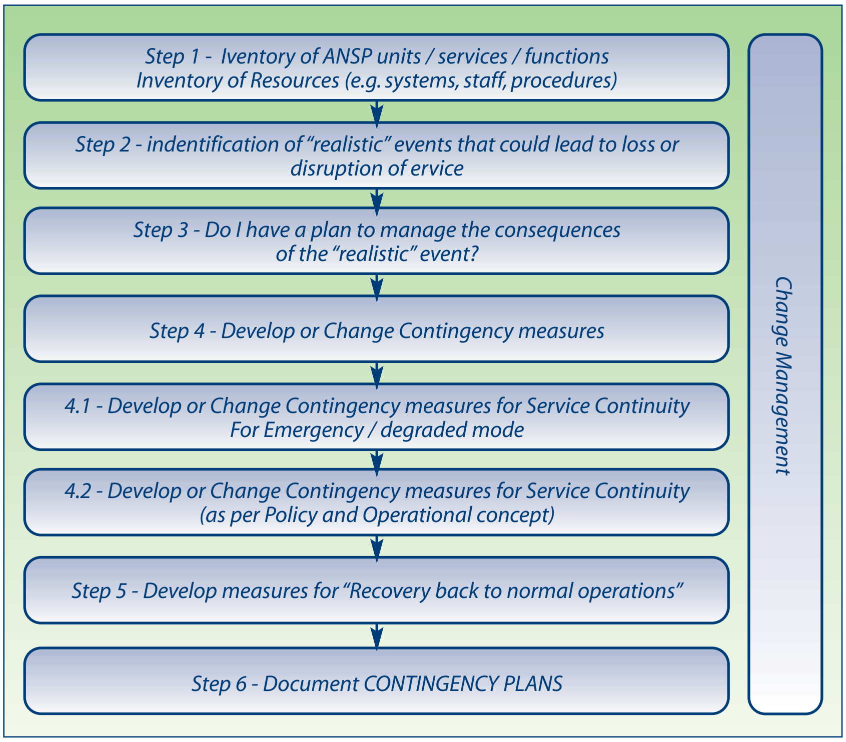

Step 1 - Iventory of ANSP units / services / functions
Inventory of Resources (e.g. systems, staff, procedures)
Step 2 - indentification of "realistic" events that could lead to loss or disruption of ervice
Step 3 - Do I have a plan to manage the consequences of the "realistic" event?
Step 4 - Develop or Change Contingency measures
4.1 - Develop or Change Contingency measures for Service Continuity For Emergency / degraded mode
4.2 - Develop or Change Contingency measures for Service Continuity (as per Policy and Operational concept)
Step 5 - Develop measures for "Recovery back to normal operations"
Step 6 - Document CONTINGENCY PLANS
Change Management

Figure 9: Overall Contingency Planning process

ruption of service or function should be identified. The likelihood of the events is to be considered to identify which ones are "realistic".

Step 3. Do I have a Plan to manage the consequences of the "realistic events"? This question is a corner stone of the contingency planning process. It is the first step to initiate the development of "contingency measures" or the "change" of existing ones. It may also lead to "re-visiting" the requirements identified at the Policy stage if it is not possible to develop a "viable" plan to meet them.

Step 4. Develop or change contingency measures - in this step, an ANSP should ensure first that safety and ATM security requirements are met. Plan(s) should be developed to deal with "Emergency" and "Degraded modes" of operation (4.1). In addition, if there is a need to ensure "Service Continuity", and if this is "viable" (in terms of policy/operations/economics), "Service Continuity" plan(s) might be developed (4.2).

The final output of this step is to develop (or to amend) the various actions to enable the implementation of the chosen contingency measures. Essentially it describes who does what, where, when and how.

For 'Emergency', 'Degraded' modes of operation and 'Service Continuity' ***Safety Assessment and Security Risk Assessment*** should be conducted: the aim of this step is to ensure that the planned contingency measures meet safety and security requirements set at Policy step.

For "Service Continuity" measures, an ***Economic assessment*** of the viability of the plan would also be required since "business" considerations are more likely to drive the development of such plan(s).

Step 5. Develop measures for "recovery back to normal operations"
Appropriate measures should be developed to ensure a safe and secure resumption or upgrade of the services after a contingency situation. Similarly a safety and security assessment of the measures should be conducted.

Step 6. Document Contingency Plans - The Contingency Plan pulls together the response of the whole organisation to total loss or major disruption of ANS service capability. Those using the plan should be able to select and deploy appropriate actions from those available in the plan and direct the maintenance and/or resumption of service units according to agreed priorities and requirements. The Contingency Plan should contain checklists of actions by nominated actors and personnel to effect contingency requirements.

A change management process should be also established to update as required the contingency plans.

STEP 1 - INVENTORY OF THE UNITS/SERVICES/FUNCTIONS OF AN ANSP

The first step is for an ANSP to identify as extensively as possible the portfolio of the services/functions it provides to all its customers. For example, at a 'service' level an ANSP may provide ATS (en route, approach and tower) which at a 'functional' level will involve provision of VCS, surveillance, FDPS etc.

Similarly, ANSPs could list all the suppliers of services and/or products whose failure may impact their delivery of air navigation services/functions:

1. List ANS Units (e.g. ACC, APP, TWR)
2. For each unit, list the services (e.g. ATS, AIS) /functions (e.g. Communication, Navigation, Surveillance, Data Processing System) provided;
3. For each unit, list the external suppliers
   3.1. of Air Navigation products and services supporting the Unit (e.g. AIS, MET, CNS);
   3.2. of other non-ANS suppliers (e.g. IT, Power supply...)

An inventory should also be made to identify the additional resources required to satisfy the contingency requirements.

Note: The Sec RAM places less emphasis on the inventory of services etc but is more focused on an ANSP's assets that enable it to provide ANS. The protection of assets is of prime importance and is in itself an end goal. In a similar way this is also true in contingency, except that within contingency it is the effects of any loss or unavailability of assets on the ability of an ANSP to provide services that is important.

STEP 2 - IDENTIFICATION OF "REALISTIC EVENTS"

STEP 2.1 - LIST THE EVENTS AND THEIR IMPACT ON "NORMAL OPERATIONS"

For each ANS unit in an ANSP portfolio, the first action is to list the events and to determine their impact on the "normal operations" (see Contingency Life-Cycle at chapter 3). Either they are not altering the "normal operations" or they lead to loss/disruption of air navigation service/function provided and/or loss or disruption of supplied services/products.

Step 2.1.1 Events not altering normal operations

Some events may occur during the "normal operations" phase that can be considered as not altering "normal operations".

Such events may have been identified during a formal safety or security assessment of the overall ATM system/service e.g. by applying EUROCONTROL SAM or Sec RAM techniques. However, within the safety elements, such a safety assessment of the overall ATM system/service may not exist. Safety assessment may only have been performed on certain parts of the overall ATM system/service along with the introduction of any changes to the overall ATM System/Service. These safety assessments of some changes of the ATM system/service do include an analysis of failure consequences on operations. The safety assessment conclusions are transferred into operations manuals that notify operational as well as technical staff the actions to be taken for certain failures. Some of these failures do not impact the normal operations because of the nature of the failure and because the ATM system/service architecture is fault-tolerant to such failures.

For the legacy part of the ATM System/service (e.g., the part not changed) for which no safety assessment was conducted, the identification of the events that will not alter "normal operations" may not have been formalised. Some of these events are either formally identified in the operations manual, even though no safety assessment supports them. Alternatively, they are made known as part of the training or made known following an occurrence via information notices (sharing lessons learned) or yet unknown.

Therefore, one action of ATM Service Providers will consist of reviewing existing material in order to assess whether adequate data are provided to draw such a "list" of events for which normal operations are not altered. The word "list" does not mean that a stricto sensu list exists as such, but suggests that this information should formally exist and be made known to appropriate staff.

The following is a list of examples events which (routinely) do not trigger an emergency/degraded mode procedure (i.e., they are part of the "normal operations" envelope):

- loss of one ODS of a sector: e.g. the sector is composed of more than one ODS and manned with at least two ATCOs both having surveillance screens;
- loss of a radar site as long as the number of remaining radars available is at least equal to the minimum number of radars required to operate a sector "normally";
- replacement of an ATCO (e.g. feeling sick) by another ATCO licensed on the sector;
- combining existing sectors (not new sectors);
- maintenance intervention on equipment for which the level of redundancy allows normal operations to be maintained (e.g. 3 levels of redundancy have been implemented though only two are necessary to operate in "normal mode" the third level of redundancy was introduced to allow such "transparent" interventions .

Step 2.1.2 Events altering normal operations

Other events may lead to loss/disruption of Air Navigation service/function provided and/or loss or disruption of supplied services/products.

<u>Process & Criteria to identify events altering "normal operations"</u>

Events may be collected through 'brainstorming' by the different technical and operational departments (including ATM Security) of the ANS unit,. This brainstorming may be supported by existing lists, "records" or "history" of events:

- Database of events/incidents (if existing);
- Benchmarking (exchange with other ANSPs);
- Systematic analysis (e.g. FHA when already done).

Events may be of different categories:

- ATM related events (e.g. extracted from existing FHA);
- Building/ANSP Infrastructure events (fire, power supply, IT);
- Environmental events (floods, earthquakes, "SEVESO like" chemical plant explosion)
- Events affecting the workforce (food poison, industrial action, pandemics)
- Security related events (terrorism, sabotage, IT hacking)
- Airborne threats (hi-jacking, aircraft crashes)

As a formal and complete list cannot be drawn up that applies to any Air Traffic Service Provision in any airspace, these guidelines are restricted to a process and criteria to specify them. However, an incomplete list covering "ATM" and "Building" related events is provided in Appendix B- List of Events to Support Risk Assessment as an example to illustrate the topic. This list is not intended to be used as such, but would have to be assessed for its suitability within any specific operational context.

These Guidelines (process & criteria) would have to be applied by ANSPs in order to assess their own existing list of such events for completeness. The guidelines may also be used to assess any existing equivalent process set-up by ANSPs in order to help them demonstrate that their existing process is robust enough by "comparison" with the recommended one.

These Guidelines will need to be customized by ANSPs to match any local specific operational aspects or additional national regulation that may influence them.

STEP 2.2 FILTERING TO DETERMINE "REALISTIC EVENTS"

For each ANS unit, the second action is to filter the "events altering normal operations" to determine which of them are "realistic" (i.e. whose probability is significant enough to be considered).

The method is mainly based on "Risk assessment" methods and may be supported by:

- Occurrence Database(s) of events/incidents (technical and operational - if existing);
- Information collected from another national agency whose expertise is specific to categories of events (e.g. Security services for Security threats, national/local authorities responsible for prevention of natural disasters°).

Realistic events can be listed by using both criteria to include or exclude them:

- Events should be considered "realistic" when:
  - the mitigation of their consequences is required as per regulation: e.g. "false fire detection alarms" when a national regulation enforces usage of sprinklers in the Ops room to extinguish fire; then a procedure (dry pipes) should be in place to manage false alarms;
  - they have been already experienced: e.g. as known by history or recorded in occurrence database(s);
  - they have been experienced by other ANSPs in a "similar" operational environment;
  - they are equivalent to another "realistic event" or linked through a chain of events.

- Events should be excluded when rationale exists that prevents them from being considered "realistic" :
  - when the event is unlikely to occur and for which no direct or indirect mitigation means exist; thus risk is considered as negligible and it is accepted: e.g. meteorite hitting ATC (if big meteorite then all staff killed and adjacent ACC may also be impacted);
  - an event is unlikely to occur (but for which mitigation means could exist); thus risk is considered as negligible and it is accepted: e.g. earthquake above a given magnitude in an area which has no records of such activity;
  - associated or equivalent to another unrealistic event.

The decision to exclude events from being 'realistic' should be documented.

The outcome of this step 2 is to obtain, for each ANS unit, a consolidated list of events that could "realistically" lead to loss or disruption of service(s)/function(s).

STEP 3 - DO I HAVE A PLAN TO MANAGE THE CONSEQUENCES OF THE "REALISTIC EVENTS"?

The third step is to review for each ANS unit, each function/service and each "realistic" event, the adequacy of the existing "contingency plan(s). From now onwards, all events considered are "realistic" and mentioned simply as "event".

The adequacy of "contingency plan(s)" means both:

- the existence of contingency plan(s) to manage the consequences of the "event" on the service/function considered;
- the contingency plan(s) meet the requirements (in terms of safety, security, capacity, environment) set at Policy level.

ANSP will face two situations: either "contingency plan(s)" exist to manage consequences of certain types of event or they do not.

STEP 3.1 CONTINGENCY PLAN(S) EXIST TO "MANAGE" THE EVENT

When "contingency measures" exist, their "performance" in terms of safety, security, capacity and environment (when relevant) is to be compared to the requirements set at Policy level:

- when requirements are met, there is no need to develop/change them (except as a consequence of the Step 5 "safety assessment/safety case").
- when requirements are not met, the "contingency measures" have to be "re-designed" to meet the requirements. It might be an iterative process.

If it is not possible to design or re-design viable contingency plan(s) to meet some requirements, the latter may have to be "re-visited" (refer Step 3.3 Re-visit requirements set at Policy level).

In any case, contingency plans must be subjected to (and pass) a safety and security risk assessments that should be documented (see Step 6) if this has not already done.

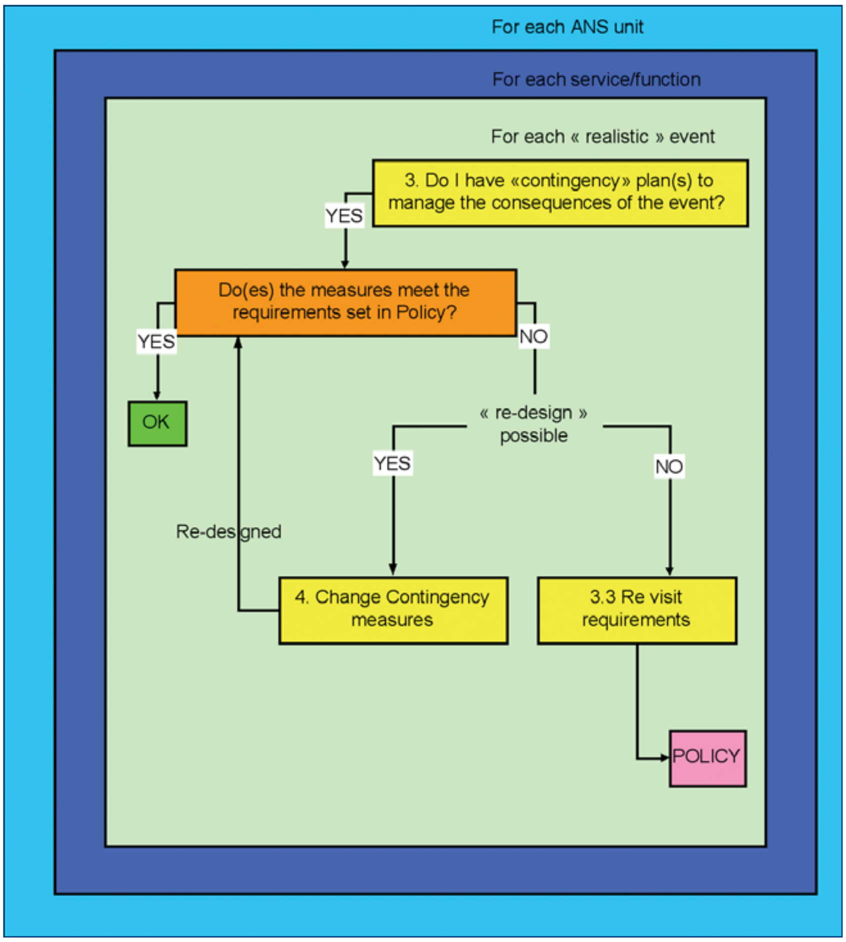

For each ANS unit
For each service/function
For each « realistic » event
3. Do I have «contingency» plan(s) to manage the consequences of the event?
YES
Do(es) the measures meet the requirements set in Policy?
YES
NO
OK
« re-design » possible
YES
NO
Re-designed
4. Change Contingency measures
3.3 Re visit requirements
POLICY

Figure 10: Process to confirm or change existing CP

STEP 3.2 NO CONTINGENCY PLAN EXISTS TO "MANAGE" THE EVENT

When "contingency measures" do not exist, an ANSP has to initiate two actions:

- Firstly, "deal with current situation" with the System "as-is" (i.e. people, procedures and equipment);
- Secondly, develop new contingency measures to manage the consequences of the event.

The only way to deal with the situation and the system 'as-is', is to re-visit the requirements set at policy level and to agree with the other parties (State authorities, Users) a temporary modification of these requirements. However, safety and security should not be compromised and should not be "traded-off" with other types of requirements such as capacity, fight efficiency.

The development of contingency measures is detailed further below. Once developed, an ANSP is in the same situation as described in Step 3.1. The performances of the new contingency measures have to be compared to the requirements set at the Policy step. This comparison may result either in a further design of the contingency measures or to re-visit the requirements.

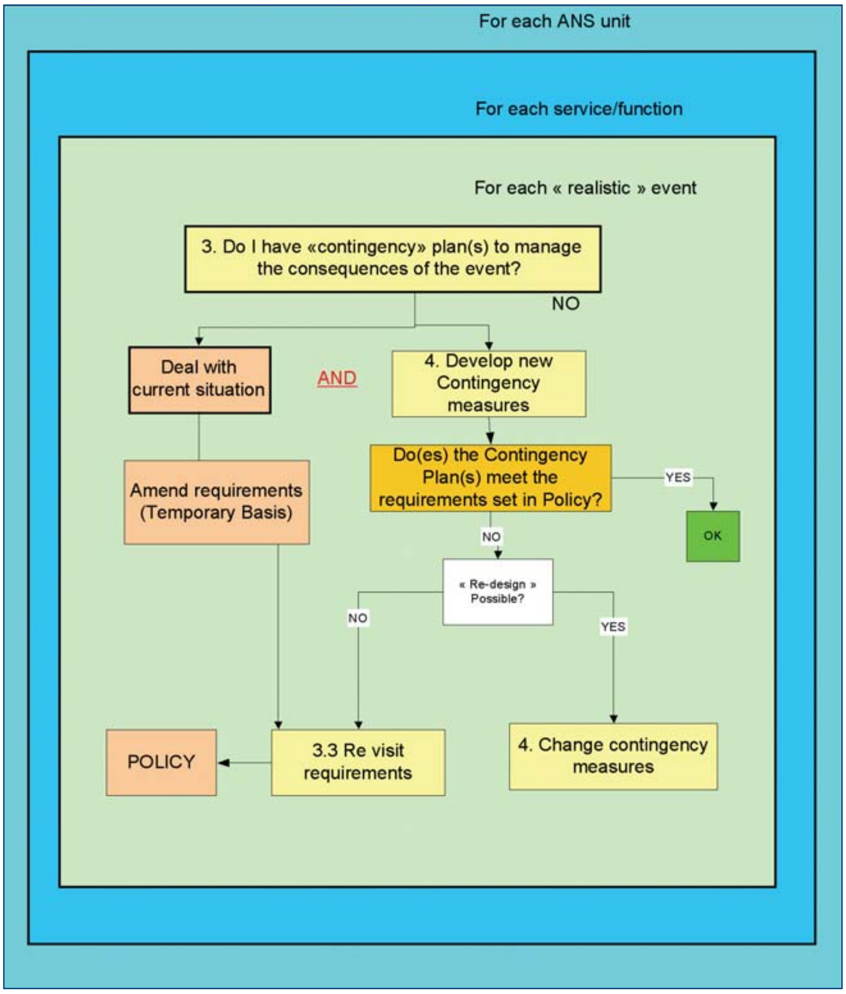

For each ANS unit
For each service/function
For each « realistic » event
3. Do I have «contingency» plan(s) to manage the consequences of the event?
NO
Deal with current situation
AND
4. Develop new Contingency measures
Amend requirements (Temporary Basis)
Do(es) the Contingency Plan(s) meet the requirements set in Policy?
YES
OK
NO
« Re-design » Possible?
NO
YES
POLICY
3.3 Re visit requirements
4. Change contingency measures

Figure 11: Process to deal with current situation and develop new CP

STEP 3.3 RE-VISIT REQUIREMENTS SET AT POLICY LEVEL

For any ANS unit, service/function and event:

- when there are no contingency measures in place to manage the consequences of the event;
- or when it has been determined that the contingency measures (either in place or developed) are inadequate to satisfy all the requirements set at Policy;

Then there is a need to re-visit the requirements in consultation with the parties identified in the Policy step.

As guiding principles:

- Whatever the reason, Safety is considered to be a 'constant'; it should not be compromised (e.g. ANSP has to ensure 'fail to safe' in emergency and degraded modes of operation);
- Security requirements should not be compromised;
- Capacity (i.e. traffic handled), flight efficiency and possibly environment (e.g. noise abatement, night operations) are possible 'variables' to manage the consequences of the event while maintaining Safety and Security. The adjustment of these variables should be done in consultation with the Airspace Users (capacity/flight efficiency) and local authorities (for environment).

STEP 4 - DEVELOP OR CHANGE CONTINGENCY PLAN(S)

Based on the safety/security criticality of the service/function, a contingency plan to manage an "event" may consist of procedures to cover:

- "emergency",
- or "emergency" and "degraded mode of operations";
- or only "degraded mode of operations".

In addition, driven by "business/corporate" considerations, ANSP contingency plan(s) for 'Service continuity' may be developed.

STEP 4.1 DEVELOP OR CHANGE CONTINGENCY PLANS FOR EMERGENCY AND DEGRADED MODES OF OPERATION

The System should be considered in all its aspects (people, procedures and equipment). Contingency measures for "emergency" and /or "degraded mode of operation" might consist of:

- development of "fall-back" systems to improve the resilience of the technical systems;
- development of "emergency" and/or "degraded modes of operation" contingency procedures to be actioned during contingency situations ;
- development, as relevant, of the "people" aspects (both operational, technical and maintenance staff) and "procedures".

Step 4.1.1. Improve the Resilience of the System

The development of "fallback" systems to improve the resilience of the system should be addressed at design stage. This aspect is not covered in these Guidelines. However, this development shall be made in compliance with the ESARRs (in particular ESARR4 and ESARR6 for Software).

However, whatever the level of resilience achieved in the System, it is necessary to develop "contingency measures" to manage the situation when the "fallback" systems fail.

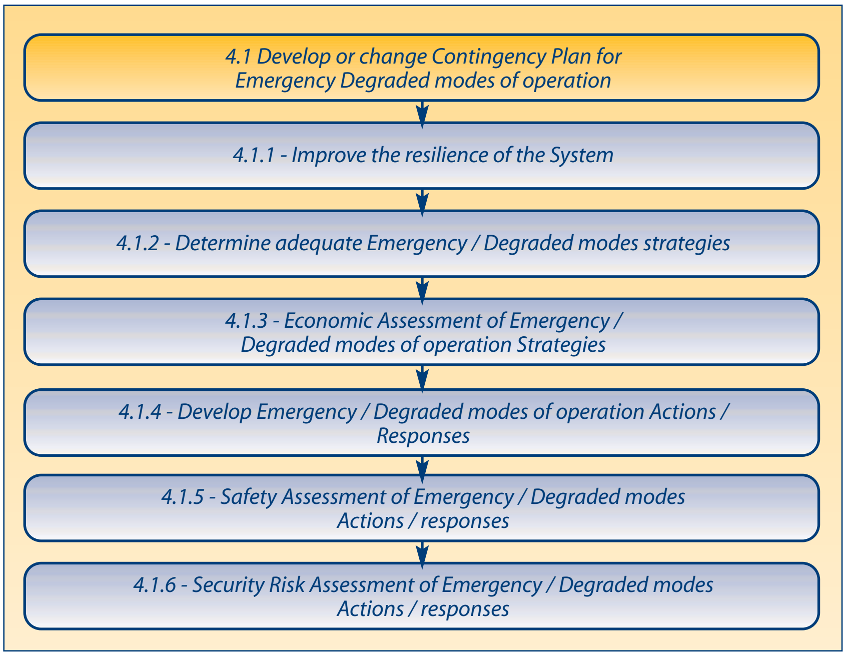

4.1 Develop or change Contingency Plan for Emergency Degraded modes of operation
4.1.1 - Improve the resilience of the System
4.1.2 - Determine adequate Emergency / Degraded modes strategies
4.1.3 - Economic Assessment of Emergency / Degraded modes of operation Strategies
4.1.4 - Develop Emergency / Degraded modes of operation Actions / Responses
4.1.5 - Safety Assessment of Emergency / Degraded modes Actions / responses
4.1.6 - Security Risk Assessment of Emergency / Degraded modes Actions / responses

Figure 12: Develop or change CP for Emergency/Degraded modes

Step 4.1.2. Determine adequate "Emergency" and/or "Degraded modes of operation" contingency strategies

The main drivers are the Safety and Security requirements identified at the Policy step. The "Emergency" and/or "Degraded modes of operation" contingency strategies should be determined and their operational/technical feasibility should be confirmed.

This phase of the contingency planning process therefore concerns determining and selecting alternative operating methods/strategies to be used after a loss or disruption of service:

- to ensure the safety of the airspace Users (Emergency situation);
- and/or to ensure a graceful degradation of the operations (Degraded modes of operation)
- and to maintain levels of ATM Security.

It should also consider protection of vulnerabilities and single points of failure in service critical processes identified during the 'filtering of realistic events' process.

In case of total outage, strategies concerning the failing unit could be either "Contingency (Alternate) Airspace strategies" or moving personnel to another location co-located or close to the failing unit (contingency (Alternate) Location strategies). Guidance is provided in Appendix C - ANS Contingency Strategies to support the decision -making process.

In case of a partial outage, strategies may be to remain at the failing unit and provide ANS with the remaining capability of the unit ("Degraded modes of operation"). In addition, the failing unit may execute strategies planned for total outage as appropriate to the situation.

Contingency strategies should also take account of mutual aid provided by or to other organisations (e.g. CFMU and neighbouring ANSPs). The rationale for all strategies and their development approach should be fully documented and the strategies kept fully up to date to reflect ANSPs' changing requirements. The appropriate senior manager (see earlier) should always sign off the contingency strategies.

In general terms, ANSPs should ensure that the contingency strategies they select enable them to discharge their ATM Security functions and responsibilities. Moreover, they should mitigate the effects of, and ensure the organisation can tolerate and recover acceptably from:

- All contingency related scenarios identified in the 'filtering of realistic events process';
- Denial of access or loss of any worksite(s);
- Denial of airspace;
- Insufficient personnel;
- Any technology failure/outage;
- Any supplier or utility failure;
- Any outsource or other service unit failure.

Contingency Strategies should also have demonstrably low likelihood of being concurrently affected by another service disruption.

Step 4.1.3. Economic Assessment of "Emergency/Degraded modes of operations" strategies

It is assumed that financial considerations are limited to the necessary actions to implement "minimum requirements" at an acceptable cost (refer Appendix H - Principles for the Contingency Plan Economic Assessment).

Step 4.1.4. Developing Contingency Planning Actions/Response

After determining the "Emergency" and/or "Degraded modes of operation" contingency strategy(ies), an ANSP has to develop appropriate actions/responses.

The aim of the various action plan(s) is to identify in advance, as far as possible, the actions and responses that are necessary and the resources which are needed to enable an ANSP to manage a loss or disruption of ANS. Moreover, the plans should provide a documented framework and process to enable organisations to resume ANS service delivery within agreed time-scales. Key requirements are:

- Clear procedures for the escalation and control of any incidents
- Communications with stakeholders Plans to resume interrupted activities (if relevant)

The development of contingency measures should be made in compliance with the ESARRs (in particular ESARRs 4, 5 and 6) and the organisation's Sec MS Policy.

The ANS related issues to be considered while developing the contingency measures are further discussed in chapter 9 ANS Related Planning Considerations.

Step 4.1.5. Safety Assessment of "Emergency/Degraded mode of operations"

An analysis of the safety impact of the Realistic Events (RE) that trigger the need for an Emergency and/or Degraded mode plan should be conducted in order to identify the parts of the ATM service and system which are 'degraded' and those which are not 'degraded'.

A risk assessment and mitigation of the 'Degraded' Mode procedure to manage such RE(s) should be made at various phases of the procedure lifecycle:

- during the procedure definition (e.g. equivalent to a FHA);
- during the procedure design (e.g. equivalent to a PSSA);
- during the procedure development (e.g. equivalent to a SSA).

Criteria to evaluate the development of procedures:

- Check existence of appropriate level of coordination between operational and technical relevant staff;
- Check that level of safety always remains acceptable (fail safe);
- Check that level of traffic is tuned to allow safe operations during the Degraded Mode of Operations (e.g. normal level of traffic may be reduced to allow managing safely degraded modes that may occur anytime including peak traffic conditions);
- Check that maximum usage and reliance of well-proven and existing practices is made.

The level of assurance should be as a minimum equivalent to the practices as recommended for Procedure Assurance Level (PAL) 4 (see SAM-SAAP) tailored to such type of procedure.

A Template is provided in Appendix D - Templates to develop contingency procedure to support the development of Emergency/Degraded mode of operation procedures. In addition an example of template usage is provided in the Appendix E - Example of application of the "Planning" process .

PROCEDURE ASSURANCE LEVEL (PAL) 4 Degraded Mode of Operations;

I PROCEDURE DEFINITION	II PROCEDURE DESIGN AND VALIDATION	III PROCEDURE DEVELOPMENT	V OPERATION
I3 Establish a proven and well-documented starting point for the definition phase ***I2*** Ensure a minimum set of quality assurance activities ***I1*** Ensure involvement of relevant operational expertise	***II3*** Ensure suitable validation ***II2*** Ensure that HMI has been assessed ***II1*** Establish an acceptable risk level (in qualitative terms)	***III2*** Ensure an acceptable quality assurance level ***III1*** Establish an Implementation Plan which includes quality assurance activities	***V3*** Ensure minimum proficiency levels ***V2*** Establish a reporting system covering occurrences relating to the procedure ***V1*** Ensure documentation control

Step 4.1.6. Security Assessment of "Emergency/Degraded mode of operations"

As with Safety, an analysis of the Security impact of the Realistic Events (RE) that trigger the need for an Emergency and/or Degraded mode plan should be conducted in order to identify the parts of the ATM service and system which are 'degraded' and those which are not 'degraded'.

A risk assessment and mitigation of the 'Degraded' Mode procedure to manage such RE(s) from a Security perspective could be made in accordance with a Security Risk Assessment Methodology.

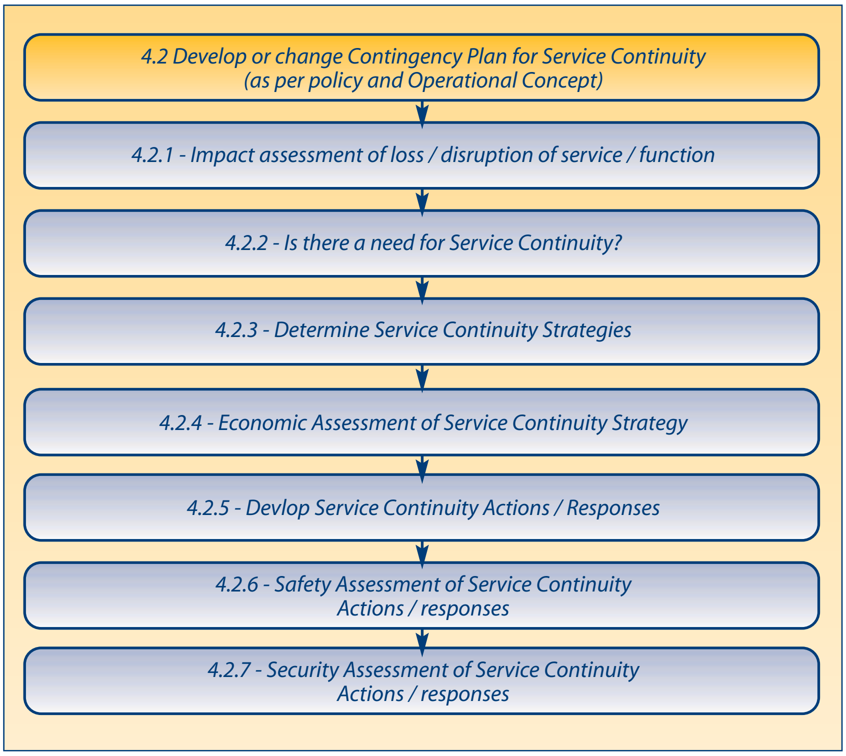
Criteria to evaluate the development of procedures:

- Check existence of appropriate level of coordination between civil/military relevant staff or those with specific ATM Security responsibilities;
- Check that level of ATM security always remains acceptable;
- Check that level of traffic is adjusted to allow, if necessary, the prosecution of ATM Security related operations (e.g air policing) during the
- Check that maximum usage and reliance of well-proven and existing practices is made.

STEP 4.2 DEVELOP OR CHANGE CONTINGENCY MEASURES FOR "SERVICE CONTINUITY"

Step 4.2.1. Impact Assessment

The Impact Assessment (IA) identifies, quantifies and qualifies the impact of a loss or disruption of Air Navigation service/function provided or any function/service supplied (e.g. IT, Power supply) so that an ANSP can determine at


4.2 Develop or change Contingency Plan for Service Continuity (as per policy and Operational Concept)

4.2.1 - Impact assessment of loss / disruption of service / function

4.2.2 - Is there a need for Service Continuity?

4.2.3 - Determine Service Continuity Strategies

4.2.4 - Economic Assessment of Service Continuity Strategy

4.2.5 - Devlop Service Continuity Actions / Responses

4.2.6 - Safety Assessment of Service Continuity Actions / responses

4.2.7 - Security Assessment of Service Continuity Actions / responses

Figure 13: Process to develop CP for "Service Continuity" (if needed)

what point in time these become intolerable in terms of safety, security, capacity, efficiency and environment. This time is mentioned later as the ***Maximum Agreed Period of Disruption - MAPD.***

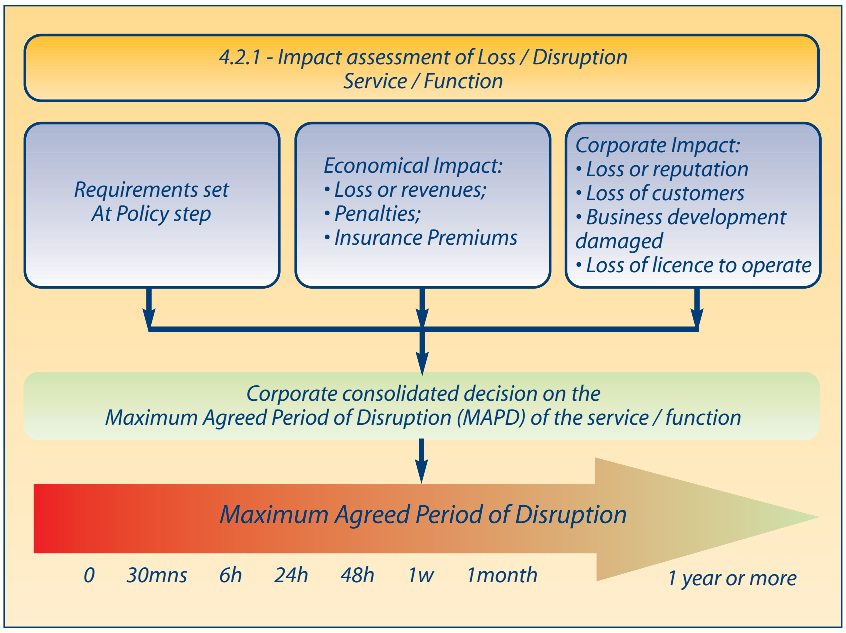

4.2.1 - Impact assessment of Loss / Disruption Service / Function
Requirements set At Policy step
Economical Impact:
• Loss or revenues;
• Penalties;
• Insurance Premiums
Corporate Impact:
• Loss or reputation
• Loss of customers
• Business development damaged
• Loss of licence to operate
Corporate consolidated decision on the Maximum Agreed Period of Disruption (MAPD) of the service / function
Maximum Agreed Period of Disruption
0
30mns
6h
24h
48h
1w
1month
1 year or more

Figure 14: Determination of MAPD

The IA should cover a number of dimensions:

1) Impact on the requirements established in Policy (i.e. safety, security, capacity, environment); for instance:

- Safety: effects on ability to provide or maintain safe ANS. The loss or degradation of system functions could impair the safety of ANS which the system provides or contributes towards, and subsequently could impact aircraft operations.
- Working Conditions: effects on ATCOs and Flight Crew ability to cope with reduction in functional capability, especially impacts on their workload.
- Adverse Operational and Environmental Conditions: effects on the ability for ATCO and/or Flight Crew to cope with adverse operational and environmental conditions
- Functional Capabilities: effects on the functional capabilities of the ground part of the ATM system and aircraft functional capabilities.
- Security: the ability of ANSPs to maintain their ATM Security obligations.

2) Impact in economical terms such as loss of revenues, penalties, insurance premiums;

3) Impact at corporate level such as loss of reputation, loss of customer, loss of licence to operate.

As part of this assessment, ANSPs should also determine at corporate level the Maximum Agreed Period of Disruption (in terms of minutes, hours, days, months) of the concerned service/function. This will have to take account of safety, security, capacity, efficiency, and environmental factors.

The process to define MAPD may be conducted through “brainstorming” sessions involving different levels of management and different departments of the ANSP to ensure as much as possible the completeness of the IA.

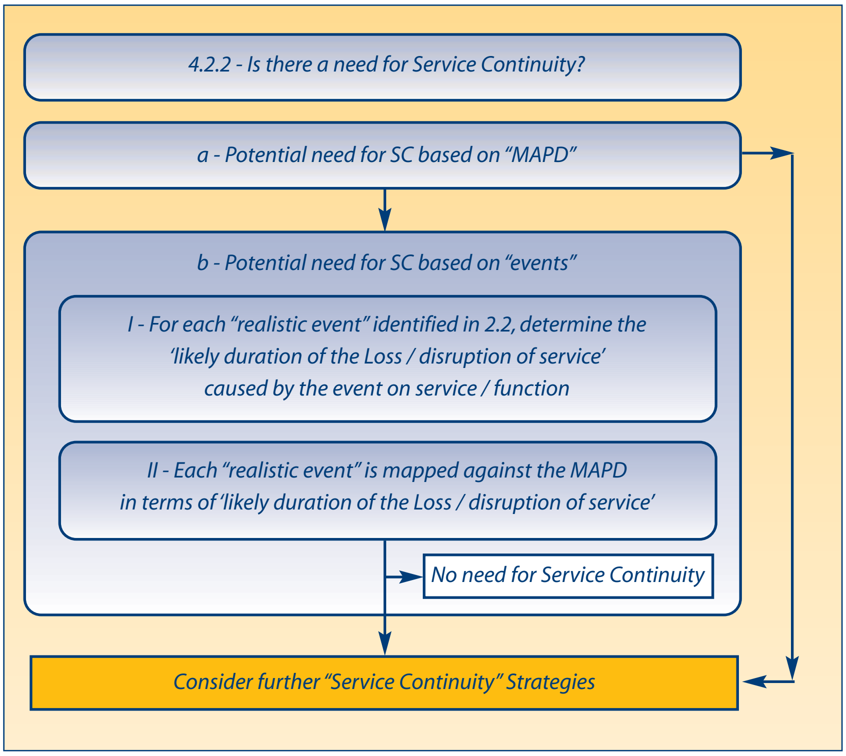

4.2.2 - Is there a need for Service Continuity?
a - Potential need for SC based on "MAPD"
b - Potential need for SC based on "events"
I - For each "realistic event" identified in 2.2, determine the 'likely duration of the Loss / disruption of service' caused by the event on service / function
II - Each "realistic event" is mapped against the MAPD in terms of 'likely duration of the Loss / disruption of service'
No need for Service Continuity
Consider further "Service Continuity" Strategies

Figure 15: Determination of need for "Service Continuity"

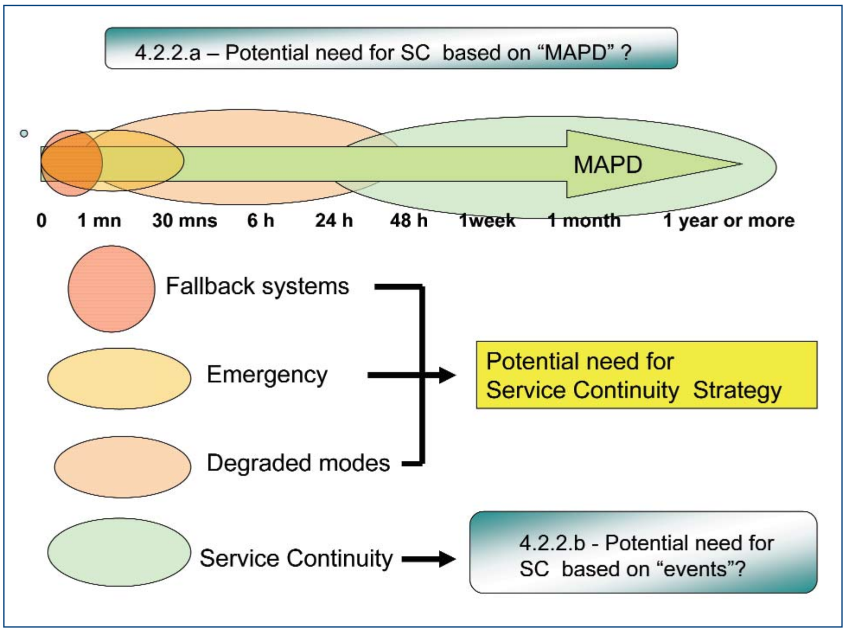

4.2.2.a – Potential need for SC based on "MAPD" ?
MAPD
0
1 mn
30 mns
6 h
24 h
48 h
1week
1 month
1 year or more
Fallback systems
Emergency
Degraded modes
Service Continuity
Potential need for Service Continuity Strategy
4.2.2.b - Potential need for SC based on "events"?

Figure 16: "Service Continuity" vs. MAPD

Step 4.2.2. Is there a potential need for "Service Continuity"?

Once the MAPD of a service/function has been defined at corporate level, it is proposed to review it along with all the "realistic events" identified in Step 2 to assess if there is a potential need to develop "Service Continuity" strategies.

a) Potential need for "Service Continuity" based on MAPD?

The first step is to conduct a preliminary identification of the potential need of Service Continuity measures based on the MAPD of the service/function.

For MAPD in terms of seconds/minutes, "fallback" systems should be developed to improve the resilience of the system. ***Their development should be addressed at design stage;*** this aspect is not covered in these Guidelines.

For MAPD in terms of minutes/hours up to an appropriate timeframe (e.g. 48 hours), "Emergency mode of operations" and/or "Degraded modes of operation" contingency measures may have to be developed in the event of a contingency situation to ensure a safe and orderly degradation of a service. Development of such measures is addressed above (refer Step 4.1 Develop or change contingency plans for Emergency and Degraded modes of operation).

However, the possibility that the service/function considered will be interrupted for longer than the agreed (MAPD) has to be considered. ***A short MAPD*** of a service/function ***indicates its importance and implies*** that this service/function is a ***potential "candidate" for further development of "Service Continuity" strategies.*** Therefore for the services/functions whose MAPD is shorter than an appropriate timeframe (e.g. 48 hours), the process of development continues.

For the services/functions whose MAPD is longer than the timeframe, the need to develop "Service continuity" plans is subject to the confirmation that there is a "case" supporting the development of Service Continuity measures.

This "case" depends on both:

- The possibility of loss/disruption of service/function for a duration greater than its MAPD; this possibility depends on the "likely duration of loss/disruption" caused by the "realistic events" identified in Step 2;
- "Business considerations" (e.g. political/operational/economical).

b) Potential need for "Service Continuity" based on events?

The possibility of loss/disruption of service/function greater than agreed is addressed in this step.

<u>i) Evaluation of the "likely duration of loss/disruption" caused by a "realistic events"</u>

For the service/function considered, the "likely duration of loss/disruption" that may be caused by a "realistic events" should be evaluated. This duration may include:

- "Exposure Time": the amount of time the event exists;
- Time for "Annunciation, Detection and Diagnosis" of the event;
- Time to Recovery back to Normal operations";
- Possible development of any additional events (cumulative aspects).
- Any time that may be caused by the enactment of "Emergency" and "Degraded modes" contingency measures;

The different times are not sequential and overlaps may exist (e.g. between "exposure time" and enactment of contingency measures).

Times may already have been evaluated in the context of the "risk assessment" performed in Step 2.2. Similar methods to collect data and to define these values could be used.

<u>ii) Mapping of the events against the MAPD of the service/function</u>

Once the "likely duration of loss/disruption of service" evaluated, each event is mapped against the MAPD of the service/function considered.

An ANSP may adopt a simple approach:

- if the "likely duration of loss/disruption" caused by any event identified in Step 2.2 is less than the MAPD of the service/function considered, there is no need for "Service Continuity" measures;
- if the "likely duration of loss/disruption" caused by one or more event(s) identified in Step 2.2 is greater than the MAPD of the service/function considered, there is potentially a need to develop service continuity measures.

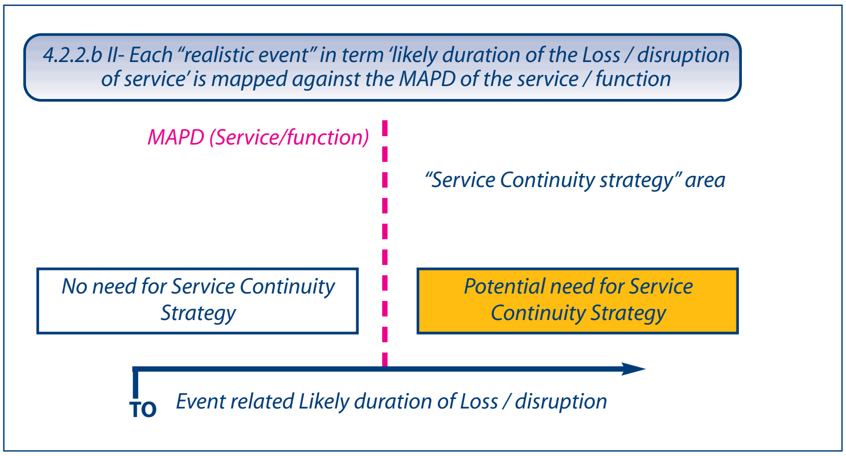

4.2.2.b II- Each "realistic event" in term 'likely duration of the Loss / disruption of service' is mapped against the MAPD of the service / function
MAPD (Service/function)
"Service Continuity strategy" area
No need for Service Continuity Strategy
Potential need for Service Continuity Strategy
TO
Event related Likely duration of Loss / disruption

Figure 17: Role of MAPD in determining need for SC

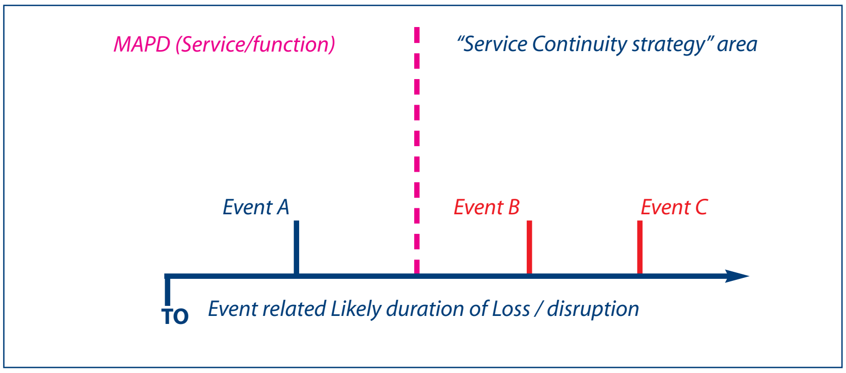

MAPD (Service/function)
"Service Continuity strategy" area
Event A
Event B
Event C
TO
Event related Likely duration of Loss / disruption

Figure 18: Example of mapping of events vs. MAPD

Note: Cumulative impact of "combination of events" in terms of "likely duration of loss/disruption" may also be considered here.

This is illustrated in the figure 18 where events B and C cause a potential need for developing "Service Continuity" strategies.

Step 4.2.3. Determining and developing "Service Continuity" Strategies

Once the need to for a "Service Continuity" strategy has been confirmed, the feasibility of suitable strategies should be further investigated.

Therefore, this phase of the contingency planning process concerns:

- identifying a range of potential Service continuity strategies;
- determining and selecting alternative operating methods to be used after a loss or disruption of service to maintain and/or resume ANS services and their dependencies (internal and external) to a priority, and time-table determined in the IA.

It should also consider protection of vulnerabilities and single points of failure in service critical processes identified in the 'filtering of realistic events' process.

In case of total outage, strategies concerning the failing unit could be either "Contingency (Alternate) Airspace strategies" or moving personnel to another location co-located or close to the failing unit (Contingency (Alternate) Location strategies). Guidance is provided in Appendix C - ANS Contingency Strategies to support the decision-making process.

In case of a partial outage, strategies may be to remain at the failing unit and provide ANS with the remaining capability of the unit. In addition, the failing unit may execute this strategy in combination with strategies planned for total outage as appropriate.

Contingency strategies should also take account of mutual aid provided by or to other organisations (e.g. CFMU and neighbouring ANSPs). The rationale for all strategies and their development approach should be fully documented and the strategies kept fully up to date to reflect ANSP's changing requirements. The appropriate senior manager's (see earlier) should always sign off the contingency strategies.

The service continuity strategies should be also economically assessed to define if there is a business case supporting the development of these strategies.

Continuation of restart capabilities need to be realistic. Physically moving staff and operations will take more time than expected and impact on the available working day. It is usually the case that the faster the recovery requirement, the greater the cost of a solution therefore, to minimise costs, it is important to ensure that service provision and capacity can resumed within a realistic reaction time.

Step 4.2.4. Economic Assessment of "Service Continuity"

It is assumed that financial considerations are one of the main drivers in implementing "Service Continuity" measures (refer Appendix H - Principles for the Contingency Plan Economic Assessment).

Economic considerations may lead either to abandoning the development of "Service Continuity" measures or re-visiting the requirements (in terms of capacity, flight efficiency during service continuity) set at the Policy level.

Step 4.2.5. Developing "Service Continuity" Actions/Response

After determining "Service Continuity" contingency strategy(ies), ANSPs have to develop appropriate actions/responses. The elements to be covered are similar to those mentioned for "Emergency/Degraded modes of operations" (refer Step 4.1.4).

The development of "Service Continuity" plans shall be made in compliance with the ESARRs (ESARR4, ESARR5 and ESARR6).

The different aspects to be considered while developing "Contingency measures" are further discussed in 9
ANS Related Planning Considerations.

Step 4.2.6. Safety Assessment of "Service Continuity"

The following should be performed:

- define different "Service Continuity" scenarios (or "Concepts of Operations") depending on the state of the "Ops System" (availability of staff, equipment, infrastructure; required traffic volume …).
- a Safety Assessment of this "Service Continuity" mode of operations using a methodology in compliance with ESARR4 (e.g. applying EUROCONTROL SAM).

Step 4.2.7. Security Assessment of "Service Continuity"

In addition to the safety assessment prescribed above, a security assessment should be performed of selected Service Continuity mode(s) of operation using a methodology such as the Sec RAM.

STEP 5 - "RECOVERY BACK TO NORMAL OPERATIONS"

The procedures for transfer "back to normal operations" should be specified.

A safety and, if necessary, security assessment of the transfer to "Normal operations" phase should be conducted in compliance with ESARR4 (e.g. applying EUROCONTROL SAM) and Sec RAM respectively.

STEP 6 - DOCUMENT CONTINGENCY PLAN(S)

STEP 6.1 CONTINGENCY PLAN(S)

The purpose of a Contingency Plan(s) of any type is to specify the detailed measures and actions that are required to enact the chosen contingency strategies. The aim of the plan(s) is to facilitate the maintenance or resumption of ANS service delivery. Those using the contingency plan(s) should be able to select and deploy appropriate strategies and actions and direct the maintenance or resumption of service units according to agreed priorities and requirements. It is recommended that the Contingency Plan(s) should be modular in design and contain checklists of considerations for action by nominated actors and personnel.

For instance, the Contingency Plan(s) (and/or sub-service level unit plans if relevant) should contain information on:

- Document owner and maintainer;
- Roles and Responsibilities of key actors;
- Invocation and mobilisation instructions;
- Action lists;
- Resource requirements;
- Essential information - contact details, LoAs etc …
- Forms/annexes - checklists etc…

STEP 6.2 CRISIS MANAGEMENT PLANS

Consistency should be ensured between Contingency Plan(s) and Crisis Management Plan(s). Crisis Management Plans will assist ANSPs to mount an effective and timely management (non-operational) response to major incidents (such as the catastrophic loss or disruption of ANS services) and thus help protect the organisation's brand from financial and reputation damage. This is achieved through the management of external stakeholders (airlines) requirements. Chapter 13 Crisis Management provides further details of Crisis Management planning considerations.

CHAPTER 9. ANS RELATED PLANNING CONSIDERATIONS

9.1 AIR TRAFFIC SERVICES (ATS)

While developing Contingency actions/responses, contingency planners should consider a number of specific Air Navigation Services related issues.

9.1.1 DELEGATION OF ATS - APPLICABLE RULES

As outlined in the chapter 5.6 Cross-border Provision of Services and Sovereignty Issues, there is a need to clarify which laws and regulations, or operational rules and procedures (e.g. which operations manual?) will be applied by an aiding Unit temporarily controlling part of the airspace of a foreign State. In application of the principle of territorial sovereignty, only the laws and regulations of the State in which the service is provided should be in force and applied.

However, it appears difficult from a practical point of view to request a foreign aiding ANSP to know and apply these rules. Should a temporary deviation from the national rules be implemented, notification should be made to the users (via AIS) and to ICAO, if it involves a difference with the Annexes to the Chicago Convention.

9.1.2 HUMAN FACTOR ISSUES (LICENSING/TRAINING)

Directive 2006/23/EC, is a means to recognise the specific role which ATCOs play in the safe provision of air traffic control. The establishment of Community competence standards which are designed to reduce fragmentation in this field, making for more efficient organisation of work in the framework of growing regional collaboration between ANSPs is particularly relevant in the context of Contingency Planning. In accordance with the principle of mutual recognition (article 15 of this Directive), States have to recognise the air traffic controller licenses and their associated ratings, rating endorsement and language endorsement issued by the NSA of another (EU) State as well as the accompanying medical certificate.

However, when ANSPs in one state may be considering the use of alternate (external) services from another state as part of their Contingency Plans it is essential that they harmonise the requirements as regards qualifications and competence of ATCOs in order to safeguard internationally accepted standards. A fundamental principle that must not be overlooked is that ATCOs are qualified to exercise the privileges of the ratings only in the sectors/Units for which they are trained. It is recognised that the Initial Training for ATCOs involves practice in the handling of Unusual/Emergency situations including for degraded systems etc. It is necessary however, to distinguish this training for emergency situations and the training needed to implement short and long term contingency measures. Further elaboration of the considerations pertaining to ATCO licensing issues can be found at 10.2 Human Resources related aspects

9.1.3 MILITARY ASPECTS

Pursuant to each State's national legislation, military concerns should be considered when drafting a contingency plan. More precisely, the exchange of basic flight (plan) data and possible continuity of service for State aircraft operations should be considered.

ATM has to support national security in respect of the identification of flights entering a State's national territory, and Air Defence organisations have to be provided with all ATM information relevant to their task. ATM also has to support day-to-day military operations through the provision of, and access to, sufficient airspace for military needs. The exchange of information between civil and military ANSPs is therefore, essential for civil-military co-ordination, and can only be achieved if civil and military systems are interoperable.

In a contingency situation, support to the Military ATS and Air Defence structures (e.g. flight planning) should continue such that support and information for the identification of flights, exchanges of information relevant to the air defence task and for interoperability of systems - air defence and contingency location - will ensure the exchange of information.

In some countries ANS is provided to military flying activities on a permanent basis by a civil ANSP. In these cases, especial arrangements should be made to guarantee the continuity of the ANS. Under contingency situations military operations shall not be compromised. Co-ordination between civil and military authorities and civil and military service providers is essential. The appropriate agreed contingency measures shall be clearly reflected in the contingency plans

The use of military premises infrastructure to support civil service continuity strategies in contingency scenarios is discussed in Appendix C - ANS Contingency Strategies.

9.1.4 AIRSPACE INCLUDING ICAO ASPECTS

For ICAO, the main objective of contingency plans is to assist in providing for the continued safe and orderly flow of international air traffic in the event of disruptions of air traffic services and related supporting services and in preserving the availability of major world air routes within the air transportation system in such circumstances. As regards industrial action in sovereign airspace it is specifically mentioned that States should "*take appropriate action to ensure that adequate air traffic services will continue to be provided to international civil aviation operations concerned, which do not involve landing or take-off in the State(s) affected*".

In cases of armed conflict and when the State concerned is not able to make contingency arrangements, ICAO would normally take the lead in preparing a contingency plan and putting it into effect. The promulgation of the plan would not be by ICAO but by a State adjacent to the area concerned. Since the airspace over a sovereign State can not be used without the consent of the State concerned, such a plan will often involve re-routing of traffic to avoid the airspace.

Contingency arrangements are temporary in nature and do not constitute amendments to the regional plan. When a contingency situation occurs very suddenly, the service provider(s) concerned should take immediate action as necessary in order to deal with the situation in the short term. However, after that initial phase there would be a need to develop or implement a specific contingency plan which, if it involves a temporary deviation from the approved regional plan, would need to be approved by the President of the ICAO Council on behalf of the Council. In particular, this would be the case when additional/new routes or route segments were to be established. In Europe, involvement of the CFMU (see 11.4 Respective roles of the ANSPs and CFMU) should ensure that any potential negative effects of airspace takeovers, closures and re-structuring on the overall European ATS network are kept to a minimum.

In the case of complete disruption of ATS there are several options:

- Re-routing of traffic to avoid the whole or part of the airspace concerned, which could involve the temporary establishment of additional/new routes or route segments. In this case it is advisable to inform ICAO at the Planning stage and it would be necessary to obtain ICAO approval immediately before Execution.

- Establishment of a new simplified route structure with a flight level allocation scheme through the airspace concerned. It would be advisable to inform ICAO at the Planning stage and obtain specific approval from ICAO before execution if it involves a deviation from the approved ICAO regional plan.

- An agreement with adjacent State(s) that the services will be provided by that State. This would normally involve a simplified route structure and reduced traffic levels. Again, it would be advisable to inform ICAO at the Planning stage. Specific approval would not be required at the Execution stage although ICAO should be informed.

In all cases, for airspace over the High Seas, ICAO should be kept informed and involved at the planning phase and ICAO approval of the contingency plan would be required before execution

These and other detailed considerations and strategies for dealing with airspace issues are contained in Appendix C - ANS Contingency Strategies as well as in Appendix J - Contingency Planning Frequently Asked Question (FAQs)- Questions 19 to 21 related to the High Seas.

9.2 ENGINEERING AND TECHNICAL CONSIDERATIONS

9.2.1 CNS GENERAL

Provision of modern-day ANS cannot be conducted at the optimum levels without the full range of CNS capability that supports the current system/network. The same range of CNS capabilities will be equally applicable to support contingency operations but will depend to some extent on an ANSP's overall approach to contingency as expressed through its Policy and Operational Concept for Contingency.

In-built technical/engineering resilience through the provision of redundant and fall-back equipment/systems should provide the necessary capability for ANSPs to deal with all but the most catastrophic engineering or technical outages and enable them to cope with Emergency and Degraded modes of Operation. However, depending on the scenario, the engineering and technical provisions for Service Continuity type operations will need to be pre-planned in line with the organisations approach to contingency. It may also be heavily dependent on the approach that it adopts to System Engineering. A number of different perspectives can be taken and some of these are described in Appendix G. Briefly, they include:

- In-House Engineering.
- Contractors and Sub-contractors.
- 'Commercial Off the Shelf' (COTS) Approaches.

- Technical Letters of Agreement.
- Cross Border Infrastructure Cooperation

9.2.2 CNS CONSIDERATIONS

It is not feasible to provide guidance on every aspect of system engineering as it would affect contingency operations. However, a list of the essential considerations covering CNS and other technical requirements is provided below.

9.2.2.1 AIR AND GROUND COMMUNICATIONS

Air/Ground Communication.

- Availability of frequencies at contingency location. - 8.33 KHz etc.
- Possible interference investigation of frequencies used at the 'failing' centre.

Ground/Ground Communication.

- Telephone and Intercom communication requirements.
- (Strip) printers and respective connections.
- Voice and data communications with airports, adjacent Centres and flow management units
- AMHS.
- OLDI connections.
- Fax

9.2.2.2 SURVEILLANCE EQUIPMENT

- Surveillance Infrastructure.
- Availability, new connections/links.
- Surveillance data sharing agreement: adaptation of existing or setting up of new agreement(s).
- Surveillance coverage requirements - evaluation of radar performance - is dual/triple coverage provided?
- Airport surveillance and detection radars.

9.2.2.3 FLIGHT DATA AND SUPPORT INFORMATION.

Flight Data Processing

- Controller Working Positions
- Sectorisation schemes - potential implications for standing procedures
- Flight data management and distribution rules
- Flight data update eligibility
- Interfaces with: IFPS, CFMU, adjacent ACCs, TMAs, TWRs, military control units

Environment Data Processing

- Environment data management and distribution rules, Environment data update eligibility.

Surveillance Data Processing

- Sensor configuration and coverage - potential implications for separation minima or type of service provided.
- SSR Code allocation - potential implications for allocation rules.

It should be borne in mind that rehearsing and managing the technical component of a contingent operation should cause fewer constraints than the constraints caused by operational considerations.

9.2.2.4 STATE SUPPORT FOR CRITICAL INFRASTRUCTURE

For some ECAC states it may be necessary to obtain state support for national critical infrastructure projects - for instance some service providers rely on communications and data cables that either pass under international waters or that have to be routed through third party states. Contingency provision may require the laying of fallback cables or the development of satellite communications channels - it can be difficult for ANSPs to implement these strategies without significant political support - for example in cases where there are regional disagreements over the communications satellite constellations that may be used to support service provision

9.3 AIRSPACE MANAGEMENT (ASM)

During partial or total outages of an ACC the FUA might be affected depending on system availability and foreseen contingency agreements. The AMC would continue with its responsibilities pending system and staff availability which might affect the access to airspace.

9.4 AIR TRAFFIC FLOW AND CAPACITY MANAGEMENT (ATFCM)

9.4.1 ROLE OF THE ANSPS RE ATFCM

Each ANSP unit should provide the CFMU with:

- Default capacity figures for individual Traffic Volumes applicable for all contingency phases.
- Their contingency airspace reconfiguration in order to enable correct flight plan distribution and relevant ATFM measures during a contingency situation.
- Lists of route availability applicable for contingency measures, including route structure and flight levels for which CFLAS eventually applies.

Further guidance is provided in 11.4 Respective roles of the ANSPs and CFMU.

9.4.2 ROLE OF THE CFMU

The pivotal role CFMU has in regulating ATFCM before, during and after a crisis affecting an ANSP is described in 11.4 Respective roles of the ANSPs and CFMU.

9.4.3 CFMU CONTINGENCY PLAN

If a CFMU crisis turns out to be a disaster, the CFMU disaster Recovery Plan is activated:

- This plan is designed to assist in restoring the CFMU operations following a disaster by relocating to the Recovery Site(s);
- During the relocation phase (maximum 24 hours), a Procedural Contingency Plan is activated. This plan is based on pre-defined and communicated Minimum Departure Intervals being implemented by the busiest Airports in Europe.

9.5 AERONAUTICAL INFORMATION SERVICE (AIS)

9.5.1 NOTIFICATION OF OUTAGES AND CONTINGENCY PHASES

When appropriate, information and procedures related to "foreseen" service outages should be diffused with a notice of one AIRAC cycle. According to Annex 15 to the Chicago Convention, § 5.1.1.1, "*A NOTAM shall be originated and issued concerning the following information:…implementation of short-term contingency measures in cases of disruption, or partial disruption, of air traffic services and related supporting services*".Therefore, the aviation community shall be informed of the contingency measures through NOTAM(s) issued as soon as possible according to the contingency phases.

9.5.2 CONTINGENCY MEASURES FOR AERONAUTICAL INFORMATION SERVICES

The objective of Aeronautical Information Services (AIS) is to ensure the flow of aeronautical information necessary for the safety, regularity and efficiency of flight. Timely, accurate and quality assured aeronautical information is a crucial foundation of the ATM system. The failure to provide timely warnings of change can adversely affect such operations. AIS operations can be broadly separated into two categories: Static data as published in the Aeronautical Information Publication (AIP) of a State; dynamic data, the publication of short notice change information by use of a Notice to Airmen (NOTAM) message.

9.5.2.1 STATIC DATA:

It is considered unlikely that a system failure in a State associated with the production and publication of AIP change information would be of lasting duration or impact. Should such a failure occur, then it is considered that the impact would probably result in the late publication of change information in paper format within the context of the appropriate AIRAC cycle. In such cases, the means of mitigation already exists through the medium of the Eurocontrol AIS AGORA interactive web-site which is already extensively used by AIS for such purposes. In passing it should be noted that ICAO does not presently recognise electronic media as a primary form of publication but changes to ICAO policy are envisaged. Nevertheless and within the context of a catastrophic failure, AIS should consider the regular off-site archiving of their AIP material.

9.5.2.2 DYNAMIC DATA:

A system outage or failure of any duration may have an impact on the timely delivery of a NOTAM with consequent impact on safety, capacity, economy and efficiency of flight. It is therefore strongly recommended that States ensure that adequate contingency plans are in place to deal with such occurrences.

- Few AIS if any have more than a single centre for NOTAM origination. If such a facility exists, then a simple Service Level Agreement (SLA) between the two centres should suffice;
- In States where independent civil and military centres exist and where the military centre issues NOTAM, then a SLA between the civil and military centres should suffice;
- Where no such duplicate facility exists, then it is recommended that AIS concludes a SLA with another AIS.
- In addition, States who are EAD Data Providers are already supported by the EAD through their Data Provider Agreement, as described in the Operational User Handbook and in the following section.
- States who are not EAD Data Providers should contact the EAB for information on the inclusion of the EAD in their contingency planning.

9.6 EAD AND AERONAUTICAL INFORMATION BUREAU (EAB)

- The European Aeronautical Database is a centralised source of Static and Dynamic Aeronautical Information. Sources of information (Data Providers) are both civil and military ANSPs, ECAC members and outside. Data Users include airlines, aircraft operators, software and product developers as well as airports and ANSPs.

- The EAD maintains contingency planning information and procedures for two main aspects: The first is an unforeseen incident (outage) at a client site that may render them unable to publish to or receive from the EAD. The second is a loss of service (outage) of the EAD. In both cases the primary focus is the exchange of dynamic data (NOTAM). In the case of urgent changes required in Static Data, these will also be published by NOTAM. Below is a description of the provisions in place for a client outage and an EAD outage.

9.6.1 GUIDANCE FOR CLIENT OUTAGE:

- Client fallback procedures for use during a local client outage are detailed in the Operational User Handbooks. In addition, the EAD helpdesk is available 24 hours a day.
- In the event of a client outage, the EAD is able to assist, and to publish NOTAM on behalf of a client for up to 48 hours after the start of the problem and the raising of an Issue by the client to the Service Desk. This does require the client to be able to maintain a communication link, whether by AFTN, telephone, fax, email or mobile telephone.
- Beyond 48 hours, clients are still required to maintain their own contingency procedures that can be put in place during those 48 hours so that the client is no longer dependent upon the EAD. In the event that a client cannot bring their contingency procedures into operation in this time frame, an extension of the provision of assistance can be requested from the Service Provider. This request is subject to approval by the EAB.

9.6.2 GUIDANCE FOR COMPLETE EAD OUTAGE:

- The contingency provision for the EAD is comprised primarily of 2 independent IT sites within Europe, and a contingency site maintained outside Europe.
- In support of this are a range of plans and internal procedures including:
- The Business Continuity Plan and Procedures mainly focus on the operational fallback scenarios to be followed by the EAD Data Operations Provider in case of unavailability of EAD core services, or loss of one of the operational sites in Frankfurt and Madrid.
- In turn, the Disaster Recovery Plan and Procedures describes all the activities to be followed by the EAD IT system Provider in order to fallback to the second or third IT centre within the required time frame in case of a complete loss of the main IT centre.
- As part of the quality assurance process, contractors are also required to show that they maintain emergency management documents that cover their staff, infrastructure, and their responsibilities to EUROCONTROL.
- The IT Service Level Specification sets out the requirements for minimum time-to-restore service for each of the EAD subsystems.
- The conclusion of the EAD Contingency Planning Task Force in 2007 supported the creation of an 'INO Light' solution, a web-based interface enabling both download by Data Users and publication by Data Providers of NOTAM. Implementation of this solution is foreseen for Release 5 of the EAD. It is a simplified version of the current provision, and will only become active in the event of total loss of the INO Data Provider Application .

9.7 MET SERVICES

9.7.1 SERVICE DELIVERY TO ATS

This version of the Guidelines focuses on the Contingency of the MET service delivery in support of ATS.

Timely, accurate and quality assured meteorological information is a crucial foundation of the ATM system and the ATS component thereof. The failure to provide timely observations, forecasts and warnings can adversely affect such operations. Since a clear separation of roles, tasks and responsibilities between ATS and MET providers exists (even when they coincide within one organisation), the way contingency is arranged should reflect these responsibilities.

A simple approach to ensure the delivery of MET information to ATS providers could be followed. By having agreements in place with the respective MET provider, the responsibility for contingency planning of the regularly delivered information rests with the MET provider i.e. the MET provider is contractually obliged to assure the delivery of the MET information. The MET provider shall put in place appropriate contingency plans for the complete service package and could recover the full costs associated with it, taking into account stakeholders' views on the relative costs and benefits of the planned mitigation measures. The ATS provider should assure itself of the suitability of the contingency plans through setting initial requirements, regular testing and review of the arrangements.

A more balanced approach is to jointly identify, between ATS- and MET-provider, which services/products are identified as critical and therefore subject to the highest order of contingency planning.

To accommodate the identification of the required service level of their (critical) MET information, a division in MET data categories could be useful. It should be noted that the supply of meteorological information could be tailored to the needs of a specific ATS unit as necessary for the conduct of its functions. Consequently, the required services and associated safety implications can vary from State to State and from Control Area to Control Area.

Warnings

Timely, accurate and quality assured meteorological warnings should be regarded as critical information crucial for the safe conduct of flight and ground operations. The failure to provide timely and accurate internationally standardised warnings such as SIGMETs (SigWX, Turbulence, Squall line, Volcanic Ash, etc.) and localised and nationally agreed warning products shall be prevented. A Service Level Agreement (SLA) between the ATS provider and the MET provider on the delivery of warnings should suffice.

Observations

To have knowledge of the current state of the atmosphere is regarded essential for flight operations. The failure of an observation system will have impact on the timely delivery of observational products provided for an airport or airspace segment. This could have serious impact on safety, capacity, economy and efficiency of flight and ground operations. Where for instance Local Routine Reports and Volcanic Ash Reports distributed locally have a clear safety aspect, the distribution to OPMET data centres of the same information has another dimension, since they are primarily used for pre-flight planning. Furthermore, it could be the case that for some ATS applications only some elements of a regulated product are seen as vital for basic operations, i.e. the elements wind, runway visual range (RVR) and QNH could be rated differently in importance than other components of an observational report. It is therefore strongly recommended that ATS providers weigh the aforementioned aspects when they discuss contingency measures and ensure that adequate contingency plans are in place to deal with system failures. A Service Level Agreement (SLA) between the ATS provider and the MET provider, clearly identifying the critical MET information and the response to system failure could suffice.

Forecasts

Where it is important to have knowledge of the current weather situation, to have knowledge of the likelihood of adverse or even hazardous weather in the (near) future is also regarded as essential for flight and ground operations. The possibility to pro-actively respond to safety related weather phenomena is highly beneficial for all ATM stakeholders. As in the case for observations, the criticality of forecasts or elements of forecast such as TAF, TREND or localised and nationally agreed forecast products is heavily dependant on the level of utilisation in the respective ATS system. It is therefore strongly recommended that ATS providers weigh the aforementioned aspects when they discuss contingency measures and ensure that adequate contingency plans are in place to deal with system failures. A sufficient means of compliance is to have a Service Level Agreement (SLA) between the ATS provider and the MET provider, clearly identifying the critical MET information and the response to system failure.

The data delivery to ATS heavily relies on the ICAO Aeronautical Fixed Services (AFS) and other approved (dedicated) means of communication. A system failure will have an impact on the timely delivery of MET information in general with the already described consequent impact on safety, capacity, economy and efficiency of flight. It is therefore strongly recommended that States, ATS and MET providers ensure that adequate contingency plans are in place to deal with such occurrences as a common interest.

9.8 AIRPORTS

Contingency planning for the airport ATC services (Terminal Approach Control, Tower ATS operations) is covered within the context of Appendix C - ANS Contingency Strategies, section Airport Facilities. In addition the following 'Airside' factors may have an influence on ATS provision: airfield pavements and CNS capabilities.

The responsibility for airfield pavements would usually fall on airport operating authorities and, consequently, they would be responsible for devising contingency plans to cope with the loss of any operating surfaces. However, ATS would have a major input in any mitigation strategies that might be conceived and ***close cooperation between ATC and the airfield operators should be maintained*** to ensure that optimal ATC solutions are found.

Similarly, the provision of CNS services related to Approach Control/Tower ATC operations may be vested in an organisation (e.g. airfield operating authorities) that is not under the managerial control of the Air Traffic Services provider at the airfield. Again, ATC should liaise closely with the appropriate CNS provider to ensure the continued availability of essential CNS services and/or the provision of alternate arrangements and procedures.

CHAPTER 10. ACHIEVEMENT

The Achievement phase verifies that the detailed means of translating the contingency plan(s) into reality are effectively in place. Specifically the phase should be designed to:

- Test, exercise and validate the planned contingency measures and thus build confidence that they could be executed and would be effective.
- Ensure that the Human related aspects are in place and ready to provide the required services in contingency situations.
- Ensure that Security measures (Collaborative Support, Airspace Security, Self-Protection) are coordinated with relevant civil and military authorities.
- Maintain preparedness for contingency situations for all involved Stakeholders.

10.1 TESTING, EXERCISING AND VALIDATION OF THE CONTINGENCY MEASURES

For the purposes of these guidelines the words 'test/testing' and 'exercise/exercising' have the following meanings in the text as adapted from the Business Continuity Institute (Business Continuity Institute Good Practice Guidelines, Version 2007.2, 15 March 2007)

- Test/Testing is usually associated with a technological procedure and/or business process (e.g. cascade system) being tried, perhaps against a target timescale. In this context a piece of equipment could be considered as a 'pass' (i.e. serviceable) or 'fail' (i.e. unserviceable). An example might be the testing of ground/ground or air/ground communications from an alternate ATM facility.
- Exercise/Exercising is normally used for a scenario-based event designed to examine decision-making abilities. An example could be a desk-top exercise to manage a major contingency causing incident.

Note: The BCI also uses the concept of Rehearsing which it describes as, "the practice of a specific set of procedures, possibly following a script, to build and impart awareness and familiarity." In these Guidelines this is referred to as Training and is covered in Section 1.2.2.

It is generally recognised that a contingency plan cannot be considered fully reliable until it has been tested and exercised as far as reasonably practical. The purpose of these activities is to confirm the validity of the planned contingency measures and help develop competence, instil confidence and impart knowledge that are essential in times of crisis. Though effort needs to be put into the technical recovery capabilities, the ***key element is the role of people and their resilience in skills, knowledge, management and decision-making.***

Ideally the validation process should be conducted making as extensive as possible use of the simulation, training or development facilities available to exercise the concept and the relevant procedures in situations as close as possible to the real life environment. Alternatively technical testing, desk checks and desk-top walk-throughs could be used. ***Given the inherent risks and safety considerations it is recognised that in most instances it is neither practical nor desirable to conduct 'live' testing, training and exercising of contingency measures where these could be detrimental to real-life operations.*** Nevertheless, it is recommended, that a planned evaluation programme is conceived to ensure that all aspects of the contingency plans have been examined as far as reasonably practicable over a period of time. The involvement of external suppliers and sub-contractors in these activities should not be overlooked and agreements should be included in contracts, SLAs etc as appropriate.

A prime objective should be to evaluate the safety of the procedures in the most critical period and sectors including the key contingency aspects identified in the Contingency Plan. With varying degrees of difficulty, several main scenarios could be evaluated; for instance:

- Simulated operations in fallback or degraded mode situations.
- Alternate services: closing (totally or partly) a failing unit and delegating (totally or partly) the provision of ATC to aiding unit(s);
- Alternate location: simulating total closure of a failing unit (evacuation of staff) and transferring totally the provision of ATC to the aiding unit(s)(with or without relocation of the evacuated staff).

The previous list is non exhaustive.

10.2 HUMAN RESOURCES RELATED ASPECTS

10.2.1 LICENSING

§ 7.2.1.2 - Human Factor Issues (Licensing/Training) - sets out the general requirements contingency planners need to consider concerning ATCO qualifications when considering the construction of contingency plans. The following section provides further detailed considerations concerning Training, Competence, and Ratings/Endorsements of ATCOs. In addition, guidance on other issues such as staff relocations is also provided.

10.2.2 TRAINING FOR CONTINGENCY MODES OF OPERATIONS.

Training for contingency planning operations is about equipping people with relevant knowledge and skills. Directive 2006/23/EC sets minimum training and medical standards for ATCOs and also requires the certification of training provision. In the context of contingency planning, personnel at both failing and aiding units should receive, as necessary, appropriate training to enable the effective execution of contingency plans. However, a distinction should be made between training for Emergency/Degraded modes of operation and Service Continuity.

10.2.2.1 TRAINING FOR EMERGENCY/DEGRADED MODES

It is essential that operational controllers and supervisors and their engineering/technical equivalents can react instantaneously to 'Emergency' events and unusual situations. Existing guidance material available to help ANSPs gauge the extent of this training includes:

- EUROCONTROL Guidelines for ATCO Common Core Content - Initial Training which lists the key operational areas to be addressed concerning the handling of Unusual/Degraded/Emergency situations.
- EUROCONTROL Guidelines for Controller Training in the Handling of Unusual Incidents can be found at: http://www.eurocontrol.int/humanfactors/public/site_preferences/display_library_list_public.html#newt11
- EUROCONTROL e-learning package can also be accessed at http://elearning.eurocontrol.int/cnr/browse.do?c=5222 .
- ESARR 5 (Para 5.2.2.6.c) states that these skills should be reinforced as necessary through "periodical refresher and emergency training".

10.2.2.2 TRAINING FOR SERVICE CONTINUITY MODES

The frequency and level of training for Service Continuity modes, however, is wholly dependent on the contingency strategies and measures adopted by the ANSP. No two situations can be the same. The extent to which ATCOs, ATSEPs, Supervisors and Managers (and perhaps external suppliers and sub-contractors) need to undertake preparation/familiarisation training for Service Continuity type operations, either as an ongoing commitment before an event or as a requirement after a contingency situation, can only be decided upon at a local level by an ANSP (supported by its NSA).

10.2.2.3 GENERAL TRAINING PROVISIONS

Consequently, the training policy for contingency should be defined at local level. There is no scope for a European or regional set syllabus (except perhaps in the context of a FAB Agreement). Where local training specifications for either Emergency and/or Service Continuity modes are defined they should be included in a Unit's Training Plan and in a conversion Training Programme as appropriate. To ensure cost-effectiveness, the impact of specific contingency training on the overall ATM personnel training and transition should be kept to a minimum.

Indeed, whatever strategies are chosen when planning contingency measures, it is recommended that to reduce the need for any additional validation training and to minimise the practical commitment, it is preferable for the contingency operation to apply the principle of '***minimal difference***' and use ***whenever possible***:

- Validated controllers from the failed site to man the contingency operation (not ruling out the possibility of cross-training at the aiding unit);
- The normal airspace structure and sectorisation;
- The normal ATC procedures;
- Identical workstation Human /Machine Interface.

Moreover, it is ***recommended*** that training should cover, as appropriate to the contingency measures foreseen to put in place:

- The contingency plan provisions at the unit in particular the Emergency and degraded modes of operation;
- "Taking over" from adjacent units;
- Special Military situations;
- Other situations as locally identified.

Training for contingency operations can be facilitated by a variety of means including briefings, simulations and joint exercises. It should take place, as necessary, during:

- Initial Training (referenced only as part of the training for emergencies and unusual situations);
- Unit Training (e.g. OJT etc.);
- Continuation Training (e.g. refresher training, including possible Conversion Training on other HMIs;
- Development Training (e.g. Supervisor/Management training).

10.2.3 COMPETENCE SCHEME

10.2.3.1 MINIMUM SKILL REQUIREMENTS AND GEOGRAPHICAL LIMITATIONS

When a unit is acting as aiding unit, its personnel should aim to provide uninterrupted ATS in a region as close as possible to the geographical limits of its own unit. Tasks originating from wider airspace delegations, deriving from ad-hoc bilateral or multilateral agreements, should be addressed as needed. To ensure uninterrupted ATS provision in case of an outage, national ANSPs should ensure their ATM personnel possess sufficient skill and experience, according to their own national standards. For instance, the language knowledge requirements set by ICAO and developed by Directive 2006/23/EC should be equally applicable in contingency operations as they are in normal operations.

Following a long term unit outage, when a failing unit's staff could be relocated to another location, the level of knowledge, skill and experience required to operate with the other location's equipment should be comparable with the one required at the failing unit and be subject to mutual, written agreement. All contingency - related courses timing, location, facilities, tools and content need to be arranged in close cooperation between a unit and its potential/agreed aiding units.

10.2.3.2 RATINGS AND ENDORSEMENTS

An ATCO licence contains one or more ratings to indicate the type of service which the licence holder may provide. Associated with the ratings are rating endorsements and unit endorsements. There are specific conditions listed for maintaining ratings and keeping endorsements valid - these conditions include the requirement for a minimum number of hours worked, competence assessment and a valid medical certificate. As in normal operations, during Contingency operations ATCOs should not provide an air traffic control service unless they hold a licence with a valid rating, including any associated rating endorsement and Unit endorsement relating to the air traffic control service to be provided and a current medical certificate of the appropriate category. Before the issue of a unit endorsement, ANSPs should ensure that provision of training for contingency measures in case of outages is covered, as necessary, in OJT and Continuation Training syllabi.

10.2.4 STAFF RELOCATION

For long-term outages (i.e. "Service Continuity" modes of operation), a pre-agreed staff relocation plan should be deployed in order to relocate the (failing unit's) staff at the aiding unit(s) as far as cost-effective considerations are fulfilled. This means that the role of the aiding unit is performed by a specified remote unit (existing or built ad-hoc) ***serviced by detached staff***.

Such an approach offers the following advantages:

- Training needs are reduced to a minimum;
- It is independent from external commitments concerning staff provision;
- Could be extremely cost effective if internal or external sharing solutions for an alternate facility are agreed.

There are also disadvantages:

- The possible trade-off between either maintaining a remote back-up or depending upon external commitment (equipment);
- There would be logistical problems to be solved;
- Costs would be simply be unbearable if internal or external sharing solution for an alternate facility were not available;
- It can work only when sufficient notice is given to move all the necessary staff, since it is neither feasible nor desirable to keep people in sufficient numbers permanently on site.

10.2.5 CRITICAL INCIDENT STRESS MANAGEMENT

Critical incidents (that may lead to contingency scenarios) can lead to stress reactions - so-called post-traumatic stress reactions - for the staff involved. Crisis/contingency intervention methods, being part of a Critical Incident Stress Management (CISM) programme, are designed to help people negatively affected by such events, to recover from these affects and return to normal functioning and behaviour. Such interventions create advantages for the staff in ANSPs and their employers because employees can return to their normal duties more quickly following an incident.

Consequently, it is recommended that ANSPs consider the use of CISM in their organisations which may be particularly relevant in the context of certain contingency scenarios. EUROCONTROL Guidelines exist to assist ANSPs implement CISM in their organisations, they are:

- Human Factors Module - Critical Incident Stress Management - HUM.ET.ST13.30000-REP-01 released on 31 December 1997.
- Critical Incident Stress Management User Implementation Guidelines released on 6 December 2005.

10.3 SECURITY (COLLABORATIVE SUPPORT AND SELF-PROTECTION)

10.3.1 COLLABORATIVE SUPPORT

In accordance with the ECAC ATM2000+ Strategy, "*ATM shall support national security in respect of the identification of flights entering a State's national territory, and Air Defence organisations have to be provided with all ATM information relevant to their task. ATM also has to support day-to-day military operations through the provision of, and access to, sufficient airspace for military needs. Moreover, the exchange of information between civil and military ANSPs is essential for civil-military co-ordination, and can only be achieved if civil and military systems are interoperable*." Consequently, security measures under the umbrella of collaborative support should be coordinated with the relevant civil and/or military authorities.

Particular attention should be paid to the preparation of contingency plans designed to handle degradations of the ATM system due to security-related emergency situations.

Among the nations, bilateral agreements have been established to deal with cross border air security incidents; contingency aspects should be addressed. At national level, coordination procedures involving air defence, ANSP and aircraft operators to deal with air security incidents have been improved; this should include the provision of contingency measures.

10.3.2 SELF PROTECTION

Regulation No 2096/2005 sets requirement on security of facilities, personal and operational data and requires ANSPs to implement a Security Management System.

Both aiding and failing units should take preventive measures in order to reduce to the minimum the delay for the relocated staff in starting their duty at an aiding unit due to security procedures. Personnel vetting is subject to national legislation/regulation, and should specify the relevant minimum security requirements for allowing people operating in its premises. Security measures under the umbrella of self-protection should be coordinated with the relevant civil and/or military authorities.

10.4 MAINTAIN CONTINGENCY PREPAREDNESS

Maintaining adequate preparedness is key to the successful execution of contingency plans. Awareness campaigns, training regimes and exercise programmes are therefore central for success. Indeed, a sustainable plan is one that has gained the commitment of the organisation and has structures and procedures in place to ensure that readiness is maintained and enhanced for the foreseeable future.

In the context of 'aiding' and 'failing' ANS units, contingency plans should clearly define:

- which "aiding" unit(s) are considered for the considered "failing" unit, depending of the contingency scenarios;
- which type of "control suites" will be used in contingency situations.

  Two possibilities could be considered regarding the aiding "Control suites" for contingency; the aiding "Control suites" could be:

  - either potential "failing type". In that case the training is limited to rehearse the different "contingency scenarios".
  - or potential "aiding unit" like. In that case, in addition, some time is dedicated to the familiarisation of the controllers to the operation of the Control suite.

The potential "aiding" and failing" units should also agree on the practical arrangements to rehearse the planned contingency arrangements and should include:

- The frequency with which the rehearsals should take place;
- The locations: specific training centre, or at the potential "falling" centre or at the potential "aiding unit".
- Depending on the location agreed, and the time of the year, taking into account:
  - availability of the training centre (if relevant);
  - spare capacity of the operational control suites (if relevant);
  - availability of the trainers and the trainees.

In addition, the training of the technical personal (maintenance of the equipment) should also be considered.

Notwithstanding the fact that all options should be considered, it would be extremely difficult to plan, rehearse and manage a contingency operation:

- During the peak hours of operation, or;
- Where a large Centre is dispersed to several small facilities.

Furthermore, since managing contingency situations is part of "Crisis management" the question of possible rehearsal of the related "Crisis management" aspects should be considered.

CHAPTER 11. EXECUTION AND ASSURANCE

This step corresponds to the execution of the contingency plan. It includes the monitoring and recording activities to be undertaken to enable the next step.

EXECUTION

11.1 INCIDENT (CRISIS / CONTINGENCY) RESPONSE MANAGEMENT

11.1.1 A DOCUMENTED PROCESS

- The roles and responsibilities of the nominated individual, teams and groups who will monitor and guide the unfolding events need to be clearly stated in Crisis Management Plans and Contingency Plans.
- The plans should contain details of the facilities that will be used by the various key players to control and manage the response. Predefined location(s) should be identified in the plans to act as crisis/contingency management centres.
- These need to be available for immediate activation and use by nominated executive/senior management teams identified in the plans.
- The centres will need to be resourced with particular attention given to the provision of adequate communications facilities to ensure that crisis/contingency situations can be managed and monitored.

11.1.2 MANAGEMENT OF THE INCIDENT PROCESS

The following process could be followed: Once receive notification of problem, the person in charge could:

- Assess situation then:
  - Either manage response through appropriate prepared plans;
  - And/or escalate to Crisis management team as per Crisis Management Plan.
- If a response is required then immediate things to consider include:
  - Are the others from whom a response is required present and able to undertake the roles assigned to them?
  - Communication of what has happened to senior management, as per Crisis Management Plan?
  - Informing operational counterparts - neighbouring units and potential aiding units (§ 11.2) - and CFMU (§ 11.4) of the situation;
  - Sending NOTAM of activation of Contingency Plan and discontinuation.
  - During the Contingency, it is essential that Users are provided with regular updates of the most recent information on the status of ATS. This may consist of, inter alia, briefings to operators by electronic means on a regular basis (e.g. NOTAMs).

11.1.3 METHODS AND TECHNIQUES

There are many Incident management methods; a generic one is suggested here.

- ***Contain*** - Is there anything that can be done immediately to stop the problem getting worse?
- ***Look*** at the Crisis/Contingency Plan - is there a pre-planned response that fits this incident?
- ***Follow*** the documented procedure which may include the following steps:
  - ***Communicate*** - trying to solve the problem on your own may waste time if the situation then gets out of control.
  - If necessary ***assemble*** a team to respond to the incident.
  - ***Assess the situation*** - find out as much as you can without putting yourselves at risk.
  - ***Predict*** the likely outcome - and adapt the Contingency Plan to provide a response strategy.
  - ***Predict*** a 'worst case' outcome - and have a 'back-up' response strategy.
  - ***Escalate*** the response to the required level within the organisation.
  - ***Execute*** the response strategy.
  - Evaluate the progress of the response against the likely outcome.
  - As soon as the situation allows, ***review*** the effectiveness of the response.

11.2 EXECUTION OF THE CONTINGENCY PLAN

A Contingency Plan may consist of the following phases:

FAIL TO SAFE

- Phase 1 - Immediate Actions
- Phase 2 - Short/Medium Term Actions (<48 hours)

SERVICE CONTINUITY

- Phase 3 - Initiation of the Option
- Phase 4 - Optimisation

RECOVERY

- Phase 5 - Longer-term Response and Recovery.

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 possible options:
- Delegation of ATS
- CFLAS.
- or 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 - neighbours and CFMU
- Consider control room evacuation, if necessary

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: Initiation of the option

Content depends on the strategy considered

For instance, actions taken in the case of a "Relocation" strategy are:

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 if necessary.
- 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.

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.

It should be noted that not all occasions will fit this model and in some situations it would be necessary to move from one phase to another non-consecutively (e.g. move from Phase 3 to Phase 5).

The following general conditions could apply:

- The condition for entering in each phase should be clearly specified;
- The responsibility for declaring the phase should be clearly specified;
- Each phase should be further broken down in intermediate steps/actions combination thereof;
- The Phase 1 (Immediate Actions) lasts approximately 30 minutes. Immediate Actions can overlap with Phase 2 (Short/Medium Term Actions).

- An "Emergency" situation always leads directly to Phase 1;
- The passage to Phase 3 (Initiation of the option) could be possible directly from Phase 1;
- The passage to Phase 5 (Recovery - Long Term Response) should be possible directly from any Contingency Phase;
- The measures to be undertaken during Phase 3 should be proportioned to the estimated duration of the outages and justifiable by mutual business considerations.
- The transfer of responsibility should be performed in the safest way;
- When possible and suitable, procedures such as CFLAS should be applied to ensure the completion of service for the traffic already under the 'failing' unit's responsibility.

11.3 RECOVERY / TRANSITION BACK TO NORMAL OPERATIONS

The Recovery phase should consist of a range of measures to transition from Contingency modes of operation to Normal Operations. It is recognised, however, that it is difficult to make definitive recovery plans in advance of contingency situations developing because of the uncertainty involved. Only when the actual circumstances have been identified as raising potential significant risks will it be possible to start making detailed plans for Recovery. Consequently, one of the first actions to be taken on executing measures (especially Service Continuity modes) is to set up a group to begin the process of planning a transition phase for recovery based on the real situation.

The aim would normally be to revert back to the pre contingency state. This could be the original unit and working positions or a new re-built facility, depending on the circumstances and the means required to restore Normal Operations. Moreover, transition should involve a coordinated declaration (aiding and failing unit) resumption of normal operations.

Further advice on these issues can be found in the EUROCONTROL publication, "A Safe Approach to Transition: Key Elements for Transition Success", SAM-SSA Chapter 3 - GMD from SAM version 2.2.

As recommended by Annex 11 to the Chicago Convention, Chapter 6.4 of Attachment C thereto, after a crisis/contingency situation has finished, it is essential that NOTAMs are dispatched as early as practicable, to notify users of the re-activation of the disrupted ATM services, to ensure an orderly transfer from contingency to normal conditions.

11.4 RESPECTIVE ROLES OF THE ANSPS AND CFMU

The respective actions of the ANSPs and CFMU before, during and after a contingency/crisis are presented in the following table.

	Role of CFMU	**Role of ANSPs**
Before a known contingency/crisis (if applicable)	● Assessing the potential impact of the crisis on the network ● Ensuring the proper coordination of any foreseen ATFCM measures. ● Planning the alleviation of the impact on AOs through any possible ATFCM solution (e.g. re-routings, Calling for more capacity from other ANSP's, etc) ● Providing awareness and communication to and with the involved as well as affected ATM partners (including AOs), through CFMU's already established communication channels.	● Providing the CFMU with all essential data, including Airspace Data, and updated capacity figures for individual Traffic Volumes applicable ● Providing the CFMU with updated lists of route availability applicable for contingency measures, including route structure and the flight levels for which the CFLAS eventually applies. ● Co-ordinating the contingency airspace reconfiguration with the CFMU in order to enable correct flight plan distribution and relevant ATFCM measures.

	Role of CFMU	Role of ANSPs
During a contingency/crisis	● Providing awareness and communication to and with the involved as well as affected ATM partners (including AOs), through CFMU's already established communication channels. ● Ensuring the proper coordination of any ATFCM measures. ● Reducing and Monitoring the demand in response to any capacity reduction in order contribute to safety (in the concerned area and in its neighbourhood); ● Alleviating the impact on AOs through any possible ATFCM solution (e.g. re-routings, Calling for more capacity from other ANSPs, etc)	● Providing the CFMU with updated capacity figures for individual Traffic Volumes applicable ● Providing the CFMU with updated lists of route availability applicable for contingency measures, including route structure and the flight levels for which the CFLAS eventually applies. ● Co-ordinating the contingency airspace reconfiguration with the CFMU in order to enable correct flight plan distribution and relevant ATFCM measures.
	Note: Safety assurance of aircraft in the affected airspace is the first consideration, regardless of what type of outage is being planned for. ATC must do whatever is necessary to assure safety, to include putting aircraft on the ground, clearing them out of the airspace, finding a way to advise the aircraft of the situation by the best means available. Once safety is assured, the situation must be controlled. This may require sterilisation of the airspace for a period of time, at least until the extent of the problem is understood. At a minimum, the volume and flow of traffic into the affected airspace must be controlled.	

	Role of CFMU	Role of ANSPs
During the recovery phase after a contingency/crisis	● Providing awareness and communication to and with the involved as well as affected ATM partners (including AO's), through CFMU's already established communication channels. ● Balancing Capacity and Demand in order to manage the Capacity increase in a safe, orderly and expeditious way.	● Providing the CFMU with updated capacity figures for individual Traffic Volumes applicable
	Note: Once ATC has the situation under control, it should begin to accommodate the traffic demand to the best of its remaining capability. The acceptable volume of traffic should be increased as conditions allow.	
During normal operations after a contingency/crisis in case of crisis/contingencies that might be reoccurring	● Facilitating ATFCM post ops analysis ● Building set of Best Practices based on ATFCM post ops analysis	● Performing local post ops analysis ● Participating to ATFCM post ops analysis ● Contribute to building set of ATFCM best practices

ASSURANCE

11.5 PREPARATION FOR ORGANISATION'S RESPONSE EVALUATION

As soon as possible after the interruption, the organisation's response should be evaluated and any necessary changes made to procedures, personnel or contracts.

To assist in the post-event analysis process, it is essential that detailed records are kept of the important decisions taken during the various phases of the contingency.

As well as any statutory and regulatory recording requirements required by national legislation, which may for example, be used in formal investigation/criminal proceedings after the event, the various contingency plans should contain checklists, logging sheets and instructions for their completion to ensure that all relevant information is captured.

If the cause of the contingency event impinged on safety and affected an ANSP's ability to provide safe ATS, then an ATM Occurrence Report should be raised in accordance with ESARR 2 requirements.

The use of proprietary crisis information management systems may also be a means to collect data for later review.

When relevant, these activities should also facilitate ATFCM post ops analysis and contribute to building set of ATFCM best practices in cooperation with CFMU.

11.6 POST-EVENT ANALYSIS

Whenever a contingency plan is exercised whether as a test or live event, it is recommended that there is an immediate debriefing meeting of senior executives and others closely associated with implementation and execution. This should be followed by a more formal evaluation of the exercise/event and preparation of a written report which details the results and the lessons identified. Thereafter an action plan could be created to implement any recommendations

11.7 MAINTENANCE OF CONTINGENCY PLANS

It is essential that Contingency Plans and the associated measures are kept up to date and maintained so that they are fit for purpose and resilient to change. This maintenance process will generally be achieved through 3 main channels:

- Review following an actual or practice event; identifying and acting upon the lessons as indicated above.
- Routine review as part of a formal change management process embedded in daily operational, managerial and business processes.
- Periodic internal and external review/audit as decided by local management and the NSA.

CHAPTER 12. PROMOTION

Contingency Planning Promotion ensures communication of the contingency culture, dissemination of lessons learnt and enables continuous improvement. ***The aim of the Promotion activities should be to embed contingency planning into ANSPs normal management and operational process;*** it should become part of the culture and not be seen as a separate activity of a specialist few. Training, testing and exercising will increase the profile of Contingency within ANSPs but a targeted awareness campaign can also help to spread the word.

12.1 AWARENESS

Although managing the contingency planning process is important, it is equally important that those who will be affected by the plans remain aware of their roles and responsibilities.

To that end, the plans should be made widely available; however, to safeguard security and commercial sensitivities, disclosure of contingency plans should follow strict 'need to know' principles in line with ANSP's corporate and national requirements.

12.1.1 AWARENESS CAMPAIGN

Like other facets of an ANSPs operational, engineering and management processes and procedures, awareness of Contingency Planning will be constantly changing as personnel join and leave the organisation. Consequently a coordinated campaign or programme can help to maintain awareness at the optimum level. The level of awareness will vary between individuals (practitioners will need to be more familiar than those who only have a minor supporting role) but the general staff requirements may include:

- Raising the alarm
- Call-out/cascade systems
- Threat response to a range of specific scenarios - fire, flood, technical outage etc.
- Evacuation drills and procedures.
- Overview of the Contingency measures.
- Inclusion of Contingency in staff induction/arrival training.

12.1.2 LESSONS LEARNED

A specific part of an awareness campaign should be the dissemination of the lessons learned from the activities listed in the Assurance step. Having identified the lessons it is essential that they are then acted upon so that the real lessons learned can be disseminated at the appropriate operational, technical and managerial levels.

12.2 CONTINUOUS IMPROVEMENT

As stated in Chapter 5 (Organisational Aspects) Contingency Planning (and execution) is not a one-man job. As contingency planning becomes embedded in the culture of an ANSP then, like in safety, all staff should be encouraged to propose solutions and suggestions (within the bounds of their competencies and knowledge) to improve the contingency provisions in the organisation.

CHAPTER 13. CRISIS MANAGEMENT

13.1 PURPOSE OF THE DOCUMENTS

An organisation's Crisis Management response can be captured in the following documents:

13.1.1 CORPORATE CRISIS MANAGEMENT POLICY DOCUMENT:

The policies and guiding principles contained in this document should be used when crisis management procedures and arrangements are formulated into individual plans. This should encourage a coherent approach and should ensure that crisis management plans for the various elements of the Organisation are consistent with each other.

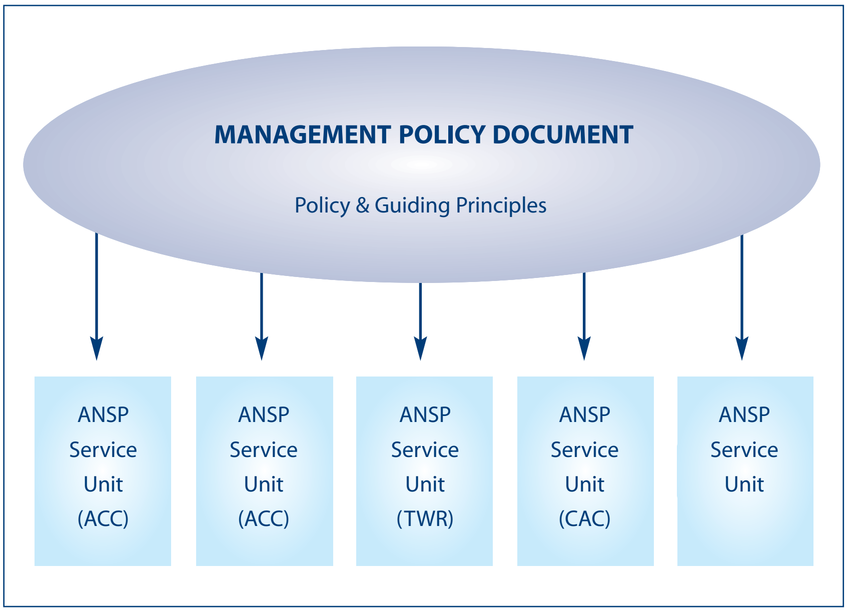


Figure 19: Crisis Management Policy and Plans

13.1.2 CRISIS MANAGEMENT PLAN(S):

The procedures to be followed in case of crisis are describes in the Crisis Management Plan(s).

13.2 HIGH-LEVEL OBJECTIVE OF CRISIS MANAGEMENT ACTIONS

A crisis situation is the result of a major internal or external event which impacts upon the Organisation in the context of public safety, staff safety, service continuity, or Organisation reputation and related public confidence (e.g. the terrorist attacks of 11 September 2001). In some cases, a crisis may be defined as an event that is not directly related to the Organisation but that is linked to its activities and that has substantial public interest e.g. failure of external supplier.

The high-level objective of crisis management actions is to identify potential, impending or actual crises and to respond to these in a co-ordinated and successful manner. Effective crisis management plans will ensure that a measured response is provided to staff, the media and to stakeholders, and where appropriate will ensure business continuity.

13.3 CORPORATE CRISIS MANAGEMENT POLICY

The Corporate Crisis management policy should address the following aspects:

1. ***Identification and notification of crises***
   Identification and notification of a crisis or potential crisis may originate from almost any source. However received, this early information must be forwarded without delay to the relevant department Crisis Management Focal Point whose role is to be defined.

2. ***Preliminary assessment of the crisis***
   On first receipt of information, the Crisis Management Focal Point should make a preliminary assessment of the crisis, and should assume responsibility for co-ordinating whatever information is available and for activating the initial stage of the relevant local crisis management plan.

3. ***Leadership during a crisis***
   Responsibilities and accountabilities must be defined and allocated without ambiguity in all crisis management plans and a clear chain of command (and line of communication) must be specified.
   In particular the role of the CEO, role of Directors/Heads of Department should be clearly mentioned.
   It is recommended to have a clearly established leadership during a Crisis. Where an event closely or directly involves an Organisation service (e.g. ACC, CAC, TWR etc), the director of that service should assume the role of Lead Director, with attendant respon-

sibility for actual running of the local crisis management plan and for keeping the CEO apprised.

13.4 LOCAL CRISIS MANAGEMENT PLANS

The different service units (e.g. ACCs, CACs, TWRs) of an Organisation are required to produce local crisis management plans based upon the policies and guiding principles contained in the Corporate Crisis management Policy.

13.4.1 OWNERSHIP OF PLANS

The owners (e.g. directors) responsible for ensuring their individual plans are current and that information contained in the plans remains valid should be clearly identified in local crisis management plans.

13.4.2 OUTLINE CONTENT

Local crisis management plans should all routinely contain the following:

Organisation related aspects

- Description of local crisis management organisation:
  1. Clear identification of Lead Director and of Crisis Management Focal Point and deputy;
  2. Crisis management teams (CMT);
  3. List of members (and deputies) of CMT with current telephone contact details;
  4. Individual roles and responsibilities;
- Procedure for liaison with CEO ;
- Location: a meeting location for CMTs should be included in local crisis management plans. Although a dedicated location may not be required, it is essential that all facilities are available in the nominated location. Plans should also identify an off-site fallback location in the event that the primary site is untenable.

Actions related aspects

- Process for notifying activation of crisis management plan and who to be notified;
- Establishing facts: it is essential the facts are gathered promptly;
- List of immediate actions with related check list;
- Service Continuity Plan; that should include the following:
  - Statement of intent;
  - Contingency location;
  - Process for assessing immediate impact of disruption;
  - Process for disseminating information immediately following disruption;
  - Process for notifying workforce of revised working arrangements;
  - Process for regular updates of information;
  - Team to operate Service Continuity (which may be different from CMT);
  - Structure of this Team, with individual roles and responsibilities;
- Recovery plan;
- Ending the crisis.

Recording and Investigation

- Details of any investigative process;
- Process for recording information: an adequate record of events (i.e. a log book) should be kept, primarily to aid the CMT but also to assist with post-crisis analysis and any subsequent formal inquiry.

Communication Aspects

- Communication with staff
- A clear link to the corporate policy for dealing with media and public inquiries.

Note: It is likely that a serious disruption of ANS will attract the attention of the media. It is essential therefore, that ANSPs are prepared to deal with media enquiries. EUROCONTROL Guidance Material for interfacing with the media in the context of Just Culture provides a wealth of useful advice that would be transferable to contingency situations. The document can be downloaded from:

http://www.eurocontrol.int/esp/public/site_preferences/display_library_list_public.html#5

Lessons learned:

- Activities to get the lessons learned of the Crisis management whenever a crisis management plan is activated - whether in practice or for real - a post-crisis audit should follow to identify lessons learnt.
- The lessons learnt should then be circulated within the organisation as relevant (e.g. to the owners of other units' crisis management plans).

Other aspects

- Other aspects where relevant, e.g. legal support.

APPENDICES TO THE EUROCONTROL GUIDELINES FOR CONTINGENCY PLANNING

(INCLUDING SERVICE CONTINUITY)

APPENDIX A - ROLES AND RESPONSIBILITIES- CHECKLIST OF ACTIONS BY STAKEHOLDERS

Details on roles and responsibilities of States (both as rule-makers and oversight authority) and ANSPs are given in Chapter 5. A checklist of actions to be completed by these stakeholders is provided below. Complimentary information concerning legal and regulatory matters is also provided in Appendix J - Contingency Planning Frequently Asked Question (FAQs).

1. STATE

- To have a good understanding of their responsibility with regard to contingency as a result of :
  - The Chicago Convention, Annex 11, Air Traffic Services, Chapter 2.30; Guidance material to Chapter 2.30, Attachment C, material relating to contingency planning;
  - The Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services, Annex I, Para. 8.2, as subsequently amended.
- To organise consultation with stakeholders in order to define specific national requirements to be met by contingency plans of respective ANSPs
- To assign national requirements on ANSPs, through regulation, or agreements; these requirements could be part of the obligations attached to designation;
- To entrust, via adequate means, the National Supervisory Authority (NSA) with the verification of contingency plans
- To approve the contingency plans (either directly or through delegation to the NSA),
- To approve the regulations/operational rules and procedures to be applied in case the contingency involves foreign ANSPs
- To approve (separately, or within the contingency plan) the agreements between ATSPs involving delegations of ATS
- To coordinate with other States concerned by the contingency plans, and if necessary conclude State-level agreements
- To coordinate with ICAO and if necessary with other international organisations; plans constituting deviations to the regional air navigation plans need to be communicated to ICAO by the State; State may need to notify differences with Annexes, if foreign regulations and procedures are applied
- To ensure publication of NOTAMs to Users when the contingency plans are applied and discontinued

2. NATIONAL SUPERVISORY AUTHORITY (NSA)

- To define, adopt and communicate to the ANSPs concerned, the NSA procedures relating to the oversight of the adequacy and content of contingency plans
- To verify the existence, content and adequacy of the contingency plans
- To define and request if necessary corrective actions in case of non-conformities
- To make arrangements for close co-operation with other NSAs in cross-border contingency conditions to ensure adequate supervision of the ANSP

3. AIR NAVIGATION SERVICE PROVIDER (ANSP)

- To develop a contingency plan in accordance with State requirements.
- To coordinate with other ANSPs, and formalise arrangements in writing
- To ensure that the written agreements with other ANSPs include provisions on the allocation of liability and on the applicable regulations and rules (e.g. operational rules),
- To review contracts with suppliers and address, if possible, contingency aspects (refer Appendix G - Systems Engineering Perspective on Contingency Strategies, § 2.2 Contractors and Sub-contractors)
- To communicate the contingency plan to the insurance companies
- To facilitate the compliance monitoring by the NSA
- To communicate to the NSA the agreements with other ANSPs (separately or within the contingency plan)
- To obtain the State's approval for agreements containing delegations of ATS (either by the State itself or by the NSA, by delegation)
- To implement/apply and execute the plan when necessary
- To disseminate information when the contingency plans are applied and discontinued

APPENDIX B - LIST OF EVENTS TO SUPPORT RISK ASSESSMENT

1. BUILDING RELATED EVENTS

This table of events is not necessarily exhaustive. It is provided to support Stakeholders in the identification of the events relevant to their services.

HAZARD REF	FUNCTION	HAZARD OR EVENT
H-BU_1	Building ATC rooms	***Total loss of ATC rooms*** due to object collision (aircraft, meteorite, vehicle...), severe damage of building
H-BU_2	Building ATC rooms	***Total loss of ATC rooms*** due to weather conditions (earthquake, tornado, lightning, wind, snow, flooding ....) leading to evacuate the personnel of the building, severe damage of building
H-BU_3	Building ATC rooms	***Total loss of ATC rooms*** due to hostile action leading to evacuate the personnel of the building
H-BU_4	Building ATC rooms	***Total loss of ATC rooms*** due to chemical pollution, leading to loss of the staff
H-BU_5	Building ATC rooms	***Total loss of ATC rooms*** due to pollution (exterior fire smoke) leading to evacuate the staff
H-BU_6	Building ATC rooms	***Total loss of ATC rooms*** due to electromagnetic irradiation
H-BU_7	Building ATC rooms	***Total loss of ATC rooms*** due to : - switch off of the Power Supply public network (failure) - strike of the Power Supply public network
H-BU_8	Building ATC rooms	***Partial loss of ATC operations due to noise***
H-BU_9	Building ATC data communication	***Total loss of ATC data*** (voice, radar, network, phone, meteorology, others FIR's)
H-BU_10	Building ATC rooms	***Partial loss of ATC rooms*** due to earthquake, vibration..., leading to a degradation of the building facilities
H-BU_11	Building ATC rooms	***Degraded conditions in ATC rooms*** due to : - turning off the potable Water Supply public network - strike of the Water Supply public network
H-BU-12	Building ATC rooms	***Degraded conditions for ATC rooms*** due to fire personnel or emergency personnel (unavailability)
H-PS_1	Power Supply ATC rooms	***Total loss of power supply*** due to : - water, fire, flood, earthquake, lightning, - equipment failures (wiring damages...)
H-PS_2	Power Supply ATC rooms	***Partial loss of power supply*** due to : - water, fire, flood, earthquake, lightning - equipment failures (wiring damages ...) - micro breakdown

HAZARD REF	FUNCTION	HAZARD OR EVENT
H-WASU_1	Water Supply ATC rooms	***Total loss of the Water Supply functions:*** Loss of the drinking and non-drinking (technical used) water supplies due to: - equipment or internal Water Supply network failures - partial loss of Power Supply - fire, earthquake
H-WASU_2	Water Supply ATC rooms	***Partial loss of the Water Supply functions:*** Loss of the drinking water due to: - equipment or internal Water Supply network failures - partial loss of Power Supply - fire, earthquake - internal Water Supply network pollution
H-HVAC_1	HVAC	***Total loss of HVAC: loss of the consoles ventilation, rooms ventilation, smokes extraction due to:*** - fire - partial loss of Power Supply - earthquake - equipment or network failure
H-HVAC_2	HVAC	***Partial loss of HVAC functions : loss of the consoles ventilation due to:*** - partial loss of Power supply - equipment or network failures - fire, earthquake
H-HVAC_3	HVAC	***Partial loss of HVAC functions: loss of the smokes extraction (in the ATC rooms and the escapes way) due to:*** - partial loss of Fire Detection - partial loss of Power supply - equipment failures - fire, earthquake,
H-FIRE_1	Fire Protection ATC rooms	***Total loss of fire Protection functions : loss of Fire Prevention, fire detection, users and equipment protection*** due to: - partial loss of Power supply - earthquake - materials degradation - partial loss of the BMS
H-FIRE_2	Fire Protection ATC rooms	***Partial loss of the Fire Protection functions: loss of the fire prevention*** (included ***equipment protection***) due to: - materials degradation or equipment failure or degradation of protection means - earthquake

HAZARD REF	FUNCTION	HAZARD OR EVENT
H-FIRE_3	Fire Protection ATC rooms	***Partial loss of the Fire Protection functions : loss of the fire detection*** due to: - partial loss of Power Supply - partial loss of the BMS - equipment failure - earthquake
H-BMS_1	BMS Office	***Total loss of the BMS office*** due to : - fire - flood altering network - network out of order (section cut-off) leading to an inability to supervise, monitor and to control the equipment of the sub-systems.
H-BMS_2	BMS Office	***Total loss of the BMS office*** due to: - partial loss of Power supply acting on BMS room
H-BMS_3	BMS Control function	***Partial loss of the BMS*** due to a loss of control functions (sub-systems elements failures, server failure, control station failures, loss of monitor functions.).
H-BMS_4	BMS Monitoring function	***Partial loss of the BMS*** due to a total loss of the monitoring function (sub-systems elements failures, server failure, work station failure...)
H-BMS_5	BMS Software	***Total loss of the BMS*** due to a bug of the software (main program generating a false alarm or unwarranted command...) - where the issue freezes or shuts down SW application,

BMS: Building Management system
HVAC: Heating Ventilation & Air Conditioning

2. ATM RELATED EVENTS

This table of events is not necessarily exhaustive. It is provided to support Stakeholders in the identification of the events relevant to their services

HAZARD ID	FUNCTION	HAZARD/EVENT
H-RDP-1.	MRT	Total loss of MRT (Multi Radar Tracker) within centre for more than X seconds (fallback available)
H-RDP-2.	MRT	Total loss of MRT (Multi Radar Tracker) within centre for more than Y seconds with fallback unavailable
H-RDP-3.	Fallback	Total loss of Surveillance fallback for more than X'
H-RDP-4.	Correlation	Total loss of track correlation for more than X'
H-RDP-5.	By-Pass	Total loss of all radar by-pass
H-RDP-6.	By-Pass	Loss of one radar by-pass
H-RDP-7.	SSR code	Total loss of SSR code management
H-ODS-1.	ODS- Maps	Total loss of maps at one ACC-CWP
H-ODS-2.	ODS- Maps	Total loss of maps at one ACC-sector
H-ODS-3.	ODS- Maps	Total loss of maps at one APP-CWP or sector
H-ODS-4.	ODS- Maps	Total loss of maps in ACC
H-ODS-5.	ODS- Maps	Total loss of maps in APP
H-ODS-6.	ODS -QNH	Total loss of QNH on APP-CWP
H-ODS-7.	ODS	Total loss of one ODS of a sector
H-ODS-8.	ODS	Total loss of all ODS of a sector
H-ODS-9.	ODS	Total loss of all ODS of a Centre
H-NET-1.	STCA	Total loss of STCA for more than 30 sec.
H-NET-2.	MSAW	Total loss of MSAW for more than 1 min.
H-NET-3.	AIWS-DAIW	Total loss of DAIW for more than 30 sec.
H-R&P-1.	REC&PLB	Loss of Record & Replay
H-FDP-1.	FDM	Total loss of FDM (Flight Data Management) for 10 min to 3 hrs

HAZARD ID	FUNCTION	HAZARD/EVENT
H-FDP-2.	FDM	Total loss of FDM (Flight Data Management) for more than 3 hrs
H-FDP-3.	CWP-FDP	Total or partial loss of 1 CWP for more than one FDP data up-date (10 sec)
H-COM-1.	A/G COM	Total loss of A/G COM for more 10 sec. of the frequency one sector with G/G COM available
H-COM-2.	A/G COM	Total loss of A/G COM for more 10 sec. of all frequencies of the centre (main, reserve, emergency) with G/G COM available
H-COM-3.	A/G COM	Total loss of A/G COM for more 10 sec. of all frequencies of the centre (main, reserve, emergency) with G/G COM unavailable
H-COM-4.	A/G COM	Partial loss of A/G COM (total loss of transmission of 1 sector) with G/G COM available
H-COM-5.	A/G COM	Partial loss of A/G COM (total loss of transmission of multiple sectors) with G/G COM available
H-COM-6.	A/G COM	Partial loss of A/G COM (total loss of reception of 1 sector) with G/G COM available
H-COM-7.	COM A/G	Partial loss of A/G COM (total loss of reception of multiple sectors) with G/G COM available
H-COM-8.	COM G/G	Total or partial loss of G/G COM for more than 10 min. one sector with A/G COM available
H-COM-9.	COM G/G	Total or partial loss of G/G COM for more than 10 min. of all G/G comm. multiple sectors with A/G COM and OLDI available
H-COM-10.	COM G/G	Total or partial loss for more than 10 min. of all G/G comm. of the centre with A/G COM available and OLDI unavailable
H-COM-11.	COM G/G	Total loss of OLDI with one centre for more than 6’
H-COM-12.	COM G/G	Total loss of OLDI with all centre for more than 6’
H-COM-13.	COM G/G	Total loss of CFMU connection
H-SUP-1.	SUP	Total loss of Operational supervision
H-SUP-2.	SUP	Total loss of Technical supervision

APPENDIX C - ANS CONTINGENCY STRATEGIES

1. GENERAL

A variety of ANS contingency strategies are available to help ANSPs move away from the high level abstraction of the Contingency Life Cycle (see Ref) and the Operational Concept towards more detailed planning of contingency measures. These strategies have been identified following site visits to a number of ECAC ANSPs and provide insights of what ANSPs are currently planning to do or have already done to prepare themselves for contingency operations. Typically, the strategies are classified as either 'alternate airspace' strategies or 'alternate location' strategies and include:

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

Detailed descriptions of each of these strategies are provided later in this Appendix. In addition, information is provided about other related issues such as cFLAS, Procedural Control, TIBA, High Seas and the use of military facilities. Appendix I- Special Cases provides more specific guidance covering a range of contingency strategies to deal with 'special' cases such as pandemics, volcanic ashes, common modes of failure (software bugs).

It is stressed that the strategies listed above are not mutually exclusive and it may be necessary to use several different approaches or combinations of approaches to meet ANSPs' needs. Moreover, depending on the type of "failing unit" (i.e. ACC, TMA, APP, and TWR) several contingency strategies might be considered when developing "Emergency", "Degraded mode of Operation" or "Service Continuity" arrangements.

The choice of strategy(ies) should be discussed in the context of the Operational Concept and as such will depend on a host of local factors including the scale and complexity of service provision, the requirements of the State and Users and the engineering/technical approach (see Chapter 9 and Appendix G - Systems Engineering Perspective on Contingency Strategies) adopted.

The table below is intended to help the decision making process while determining the appropriate "Contingency strategy". It presents the possible "Contingency strategies" available to "failing ANS units" (i.e. ACC, TMA, APP, TWR) linked to "contingency phases" (i.e. Emergency (EM), Degraded modes of operation (DG), Service Continuity (SC)).

	CONSIDERED FAILING UNIT			
Contingency Strategies[1]	**ACC**	**TMA**	**APP**	**TWR**
ALTERNATE AIRSPACE STRATEGIES				
Closure of airspace and re-routing	EM/DG/SC	EM/DG	EM/DG	EM/DG
Simplified route structure/CFLAS	DG/SC	DG/SC	EM/DG	
ATS delegation	DG/SC	DG/SC	DG/SC	
TBA (Traffic Information Broadcast)	DG			
Re-assignment of ATS delegation over High seas	SC			
ALTERNATE LOCATIONS STRATEGIES				
Moving personnel to Locations within same State				
other ACC (within same State)	SC	DG (if ACC/TMA co located) SC		
other TMA	DG (if ACC/TMA co located)/SC	SC	DG (proximity APP-TMA)/ SC	
other APP		DG (proximity APP-TMA)/ SC	SC	
TWR at national airport			DG (if possible)	
Military units (ATS and/or Air defence)	SC			
ATS Training/ development unit/ Simulator	DG (if ACC is co located)/SC	DG (if TMA is co located)/ SC	SC	
Common Contingency Centre (for hosting State)	SC	SC	SC	
Mobile TWR				DG/SC
Old TWR on same airfield				EM/DG (if old TWR equipped)/ SC

EM: Emergency
DG: Degraded mode of operation
SC: Service Continuity.

[1] The different "Strategies" are detailed in this Appendix to support the use of the table provided.

	CONSIDERED FAILING UNIT			
Contingency Strategies[8]	**ACC**	**TMA**	**APP**	**TWR**
ALTERNATE LOCATIONS STRATEGIES				
Moving personnel to Locations within adjacent State(s)				
Other ACC	SC	SC		
TMA	SC	SC		
Common Contingency Centre (for other States)	SC	SC		

EM: Emergency
DG: Degraded mode of operation
SC: Service Continuity.

2. FROM THEORY TO PRACTICE

A lot of work is required to go from the high level abstraction of the Life Cycle and Operational Concept to the more detailed plans that should be prepared by individual ANSP. 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."*

The strategies listed in 1.1 have been devised to close this gap. During visits to ANSPs , it was possible to identify the level of detail that is required in particular contingency documents. However, 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 abstractions in the Contingency Life-Cycle and Operational Concepts.

3. GENERIC REQUIREMENTS COMMON TO CONTINGENCY STRATEGIES

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. By combining information gathered during site visits it has been possible to devise a Contingency Framework that lists the generic requirements that are common to the contingency strategies described later in this Appendix.

The aim is to present the potential contingency strategies to help ANSPs' decision making processes in particular 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. Moreover, 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. The approach adopted by particular stakeholders will often be determined by local constraints. A SWOT analysis of each strategy is also presented that brings together the Strengths, Weaknesses , Opportunities and Threats that can be associated with each strategy.

One critical element that should not be under estimated is the role and ability of engineering and technical support to support the contingency strategy and resulting measures. Appendix G - Systems Engineering Perspective on Contingency Strategies provides additional guidance on this important aspect of contingency planning. Similarly, it is important to consider the ways in which external resources can be secured, for instance, from sub-contractors and other maintenance organisations both during degraded modes of operation, as service providers work to rectify a potential problem, and after any contingency has been declared.

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

PLANNING Preparations of Plans, covers some of the basic ingredients needed to build a contingency plan - for more detail see the 'Policy', 'Plan' and 'Achievements' sections in these 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 ' 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 these "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. 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 Assurance and Promotion sections of these 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" Chapter 9 and Appendix G

The Generic Requirements as shown in the Contingency Framework could involve all or some of the following points:

[2] 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.

[3] For the context of this document only, 'clear the skies' is understood to be 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.

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.
  - Liaise with sub-contractors and infrastructure providers.
- 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'
  - However, and if time permits, systems engineering teams and sub-contractors could be consulted to determine if they can resolve a failure before this critical decision is taken.
- 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: Initiation of the option

Content depends on the strategy considered

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 20: Generic Requirements of the Key Phases in the Execution of Contingency Plans

4. 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.

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 configuring 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.*
- There are clear vulnerabilities for co-located systems that arise within particular ECAC states.
  - *For instance, it can be difficult to identify appropriate sites that would not be vulnerable to seismic activity; similarly, for other ANSPs, co-located centres may create common vulnerabilities from flooding.*
  - *For most service providers, there is a concern that primary and fallback facilities might both be affected by any future aviation accident if they were also located close to an airport*

[4] 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
● 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
● 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)
● 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: initiation of Co-Location:
● Any relocation should be minor in terms of physical move to Co-Located facilities. ● 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
● 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
● Release shared resources

Figure 21 : Case Study of a Solution using Co-located Facilities for Contingency Planning

SWOT ANALYSIS

STRENGTHS	WEAKNESSES
● 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).	● 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. ● *Resource cannot be used for 2 purposes at the same time, might induce delay.* ● *Contingency systems may be needed to debug failure during contingency.* ● 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. ● *'Certification' of military facilities should be considered.* ● 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**
● 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.	● Could be difficult to sustain if seen to undermine the advance and facilitation of FAB and SESAR concepts and objectives.

5. 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.

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.

SPECIFIC REQUIREMENTS
PLANNING
Preparation of Plans
● Establish Multi-Use facility. ● Establish agreements with other user groups for training time and access for contingency purposes.
FAIL TO SAFE
Phase 1: Immediate Actions
● Inform other users of a Multi-Use of a potential incident. ● Obtain management permission for potential requisition of shared resources. ● Take initial steps to reconfigure the Multi-Use 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 Actions (<48hrs)
● Complete configuration of Multi-Use facilities. ● Initiate contingency for security/facilities management etc at Multi-Use site ● Establish back-ups for other users of Multi-Use resource, especially systems teams and training for watches to back-up initial users of contingency facility. ● Depending on contingency plan for gradual hand-over to Multi-Use.
SERVICE CONTINUITY
Phase 3: initiation of Multi-Use Facilities:
● Any relocation should be minor in terms of physical move to adjacent site. ● Sectorisation changes may be needed if Multi-Use facilities have fewer positions/resources than primary site. ● Ensure systems team validate reliability of data and communications infrastructure not just as Multi-Use facility goes live but also during initial operation. ● Secure lines of command and management by only allowing necessary staff to remain on-site.
Phase 4: Optimisation at Multi-use unit
● Bring in additional staff to ensure adequate rest and rotation of watches. ● Training of additional staff on Multi-Use facility to aid shift rotation etc.
RECOVERY
Phase 5: Longer-term Response and Recovery
● Release multi-use resources

Figure 22: Case Study of a Solution using Multi-Use Facilities for Contingency Planning

SWOT ANALYSIS

STRENGTHS	WEAKNESSES
● 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.	● 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. ● *Potential delays in switching to contingency configuration.* ● *Resource cannot be used for 2 purposes at the same time, might induce delay in re-configuration.* ● *Contingency systems may be needed to debug failure during contingency* ● 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**
● May also help to improve training/simulation facilities at same time.	● Could be difficult to sustain if seen to undermine the advance and facilitation of FAB and SESAR concepts and objectives.

6. 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.

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.
- Staffs 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

- 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

- 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

- 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: initiation of Centralised (national) facilities

- 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

- 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

- Review impact of contingency plans on other units as well as failing centre in terms of safety, security and operational performance.

Figure 23: Case Study of a Solution using Centralised (national) facilities for Contingency Planning

SWOT ANALYSIS

STRENGTHS	WEAKNESSES
● 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.	● 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**
● Provides a resilient approach with the potential for State backing where significant security risks exist.	● Possible internal social and politics concerns may arise within ANSPs if the central site can take over responsibility for their traffic under contingency operations: ● *Social concerns: employees in other sites may feel threatened in their activity.* ● *Political concerns about the status of neighbouring centres.* ● 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.

7. 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.

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.*
  - *There is a need to coordinate the work of internal support staff within ANSPs and also the different subcontracting organisations that may be used to maintain common systems between different ECAC states*
- 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.

SPECIFIC REQUIREMENTS

PLANNING

Preparation of Plans

- Establish political and regulatory support for Shared Common Systems (International).
  - *In such case, early engagement with Regulator/NSA is essential to clarify any international regulatory issue.*
- Establish shared common centre
- Ensure centre has software, documentation for each national site to be covered etc.

FAIL TO SAFE

Phase 1: Immediate Actions

- Inform the Aiding ATS unit of a potential incident.
- Take initial steps to reconfigure the contingency facility(ies).
- Alert other potential end users - they may lose their fallback systems if they are shared with the Failing unit.
- Use other users of shared common centre to 'clear the skies' if necessary

Phase 2: Short/Medium Term Actions

- It will be hard for any shared common centre to help in clearing the skies unless qualified staff are on-site.
- Depending on contingency, confirm delegation of responsibility to shared common centre for Phase 3 on at national regulatory level.
- Complete configuration of the shared common site for relocation.
- Initiate contingency for facilities management at shared common site.

SERVICE CONTINUITY

Phase 3: initiation of Shared Common Systems

- Ensure systems and ops staff are dispatched to shared common centre.
- Likely to be some changes in sectorisation and flow at least during initial start-up of shared facility.
- Consider relocation of national regulatory agency as well as ops and sys teams with support from host regulator.
- Predetermined lists used to determine who will remain behind to help in recovery of failed unit.
- Verify exchange of flight data etc.

Phase 4: Optimisation of Common System

- Transfer of additional staff to shared common centre to ensure adequate rest and rotation of watches.
- Training of additional staff on shared facility to aid shift rotation etc.

RECOVERY

Phase 5: Longer-term response and Debrief

- Inform all users of shared contingency centre both of the diagnosis for the incident and plan for recovery.

Figure 24: Case Study of a Shared Common Systems Solution to Key Stages of Contingency Planning

SWOT ANALYSIS

STRENGTHS	WEAKNESSES
● 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.	● 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**
● Development of shared facilities, practices, procedures and processes may provide synergies in the move towards FAB and SESAR concepts and objectives.	● 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.

8. 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 standard contents, relevant to contingency provisions, to be included in an International Agreement (e.g. LoA) can also be found in the Appendix F - Check list of provisions to include in contingency agreement between ANSPs

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, e.g. a simplified route structure and reduced traffic levels. These may be characterised as:
    - *Vertical takeover. A vertical takeover is a situation in which the role of the aiding unit is performed by one or more adjacent ANS units. ATS delegation is granted to the aiding unit to provide ATS above or below a specified FL/altitude, e.g. for high level over flights only;*
    - *Horizontal takeover. A horizontal takeover is a situation in which the role of the aiding unit is performed by one or more adjacent ACC(s). ATS delegation is granted to the aiding unit(s) to provide ATS in specified volumes of airspace, e.g. in FIR/UIR, sectors etc.*
- 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 - see Para 10.1for more information.

Overall, whilst theoretically possible, ATS Delegation to neighbouring states is a difficult option and the complexity of issues to be resolved and the workload involved need to be clearly understood.

[5] LoAs are administrative arrangements which are signed at ACC's level on the basis of prior international agreements between the States concerned. LoAs are therefore distinct from State-level agreements.

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

- Establish political and regulatory support for ATS Delegation approach supported by LoAs.
  - *In such case, early engagement with Regulator/NSA is essential to clarify any international regulatory issues*
- 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

- 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

- 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: initiation of ATS Delegation (International/ Cross Border) for Contingency.

- 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

- 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

- Identify protocol and timescale for handing back to failed unit.

MAINTENANCE OF PLANS

- 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 25: Case Study using ATS Delegation (International/ Cross Border) for Contingency

SWOT ANALYSIS

STRENGTHS	WEAKNESSES
● A relatively low cost means of maximising existing resources.	● 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. ● *LoAs are often little more than statements of intention and lack detail that is necessary in contingency situations.* ● *Hard to know what can be achieved with different SOPs/equipment etc.* ● 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**
● Development of ATS delegation practices, procedures and processes may provide synergies in the move towards FAB and SESAR concepts and objectives.	● 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. ● *Airspace users may also decide to re-route their operations through the neighbouring State if the disruption continues, leading to loss of revenue.* ● 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.

9. 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..

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
● 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.	● 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**
● 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.	● 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.

10. OTHER STRATEGY CONSIDERATIONS

In addition to the preceding potential ANS Contingency strategies, there are a number of other considerations and measures that were not covered, or only partially covered, in the detailed descriptions. Amplifying comments are provided below.

10.1 CAPACITY ISSUES

Potential capacity is a tool which may be used to evaluate the various strategy options. Assessment of remaining capacity at a failing unit or the capacity provided by aiding units is a key consideration.

Issues affecting capacity include:

- Available work stations/positions.
- Expanding possibilities (area of responsibility) of aiding sectors.
- Cooperation of aircraft operators in consolidating flights to maximise load factors.
- Exploit available capacity in adjacent or other airspace (important role to play by the CFMU).
- Adjusting military flying activities.
- Possible relaxation of environmental constraints to ease the traffic flow.

10.2 CLOSURE OF AIRSPACE AND RE-ROUTEING

Short-term "closures " of airspace may be necessary in emergency and degraded mode situations to ensure safety and/or to cope with the immediate effects of a developing scenario. Remedial tactics such as emergency dispersal of traffic, grounding aircraft and strict flow control measures can be employed to bring situations under control.

In some other circumstances, e.g. crisis/conflict scenarios, it may be necessary for airspace to be closed for longer periods of time. In these cases re-routing solutions would need to be found and within Europe, action is normally taken by the CFMU in coordination with adjacent States. It could also be considered beneficial to develop a contingency plan to by-pass the airspace concerned. Such a plan would, of necessity, involve the ANSPs in neighbouring States who would handle the additional traffic within their own airspace. ICAO should also be informed as necessary.

10.3 PROCEDURAL CONTROL

The high volume of traffic, and the complexity and configuration of airspace across ECAC makes the provision of Procedural Control extremely problematic particularly in congested areas of en route airspace. In less congested areas and for TMA/Approach Procedural Control could provide a limited capability provided that ATCOs are properly trained and endorsed; continuation training will be necessary to maintain the special skills and validity of the appropriate endorsement/rating.

10.3.1 SIMPLIFIED ROUTE STRUCTURE - cFLAS

In developing a simplified route structure the number of crossings of ATS routes should be minimized. This should facilitate the establishment of a contingency Flight Level Allocation Scheme (cFLAS) which would provide for crossings that are vertically separated. In addition, procedures applicable to ATS units, pilot operating procedures and communication procedures (including TIBA - see 10.4 below) could be developed. For example it should be specified in the contingency plan that aircraft are to maintain the assigned level and speed assigned by upstream ATS units throughout the flight through the affected area except in cases of emergency and for flight safety reasons or as instructed/advised by the appropriate ATS unit. Furthermore, the plan should elaborate (from the Operational Concept) which services (e.g. FIS and Alerting as the minimum), would be provided in the affected areas. Anticipated ATS sectorisation and associated capacity/service provision levels and acceptance of flight criteria (including emergencies and medical flights) should also be described. Meteorological conditions (hazardous weather) should also be monitored in the affected airspace and airspace users informed accordingly.

10.3.2 PROCEDURAL CORRIDORS (AIRPORTS)

The cFLAS system described above would generally not allow departures and arrivals from airports within the area concerned. However, in some circumstances it may be possible to design procedural "corridors" to and from some airports, with the help of ANSPs of neighbouring states. The viability of these arrangements will be based around a host of factors such as the proximity of the selected airport to a country's borders and the ability of neighbouring states to offer assistance.

10.4 TRAFFIC INFORMATION BROADCAST BY AIRCRAFT (TIBA)

When there is a temporary disruption of normal air traffic services the introduction of traffic information broadcasts by air-

[6] It is recognised that ANSPs cannot "close" airspace per se - that is a matter of State concern. However, for the purposes of these Guidelines "closure" is viewed as the ANSPs decision not to provide ANS in airspace affected by a contingency event (although it may be possible for aircraft to fly VFR in uncontrolled airspace).

craft (TIBA) could also be contemplated and specified in the contingency plan. Such broadcasts are intended to permit reports and relevant supplementary information of an advisory nature to be transmitted by pilots on a designated VHF frequency for the information of other aircraft in the vicinity. The State concerned should promulgate the designated TIBA airspace, the frequency to be used (which should be a frequency normally used for the provision of ATC within that airspace). The TIBA pilot procedures are described in Annex 11 to the Chicago Convention - Air Traffic Services, Attachment C.

10.5 HIGH SEAS

Provision of ANS contingency measures over 'High Seas' areas remains the responsibility of the State(s) normally responsible for ANS provision - see ICAO Annex 11 Attachment C. In most cases contingency measures will involve a variation of the level of services; such changes are considered as a temporary deviation to the approved regional plans, and therefore require the approval of the President of the ICAO Council. In addition, should a State not be able to provide the agreed services over the high seas it would be the prerogative of the ICAO Council to temporary reassign the responsibilities to provide services in order to ensure continued use of that airspace. In addition, ICAO Assembly Resolution A36-13, Appendix M - Delimitation of Air Traffic Services (ATS) Airspaces, Associated Practice 2 states: "The Council should encourage States providing air traffic services over the high seas to enter, as far as is practicable, into agreements with appropriate States providing air traffic services in adjacent airspaces, so that, in the event the required air traffic services over the high seas cannot be provided, contingency plans, which may require temporary modifications of ATS airspace limits, will be available to be put into effect with the approval of the ICAO Council until the original services are restored."

10.6 AIRPORT FACILITIES

States' airport approach control units are, generally, very much smaller than ACCs and can provide only a fraction of the lost capacity. Their facilities are not identical and the infrastructure to control en-route radio channels, etc is unlikely to be in place. The situation is likely to worsen as approach control facilities at the major airports are subsumed into Combined Approach Control (CAC) facilities.

While approach control units can provide important contingency air traffic services, especially in an enlarged area contiguous to the airport, it is unlikely that they could provide a satisfactory full replacement capability for an ACC. A mix between an aiding ACC and certain major approach control units is a possible planning scenario. It must be kept in mind however, that the more small facilities are involved the more difficult it is to plan, rehearse and manage a contingent operation.

10.7 MILITARY ATC FACILITIES

In the cases where a military unit is co-located with civil ATC Operations it may be possible to develop an agreement to transfer military ATC operations to other units in contingency situations. However, if evacuation of a failing civil ATS unit was necessary, then a co located military unit would also probably have to be evacuated.

Invoking these arrangements and freeing the military ATC facilities for essential civil contingency use raises issues such as:

- The need for Governmental agreement in principle and on any occasion when arrangements need to be activated. Hence, State Military Authorities must be consulted during the setting of the requirements for contingency operations;
- The need for military ATC to use common workstations which can support civil ATC functions;
- The need for levels of building, plant and system integrity suitable for civil operations;
- Limiting the capacity to that which can be safely handled.

In principle each of these issues can be resolved and the use of military units to supplement civil contingency capacity can offer benefits in some cases.

10.8 MILITARY SITES

Depending on the State concerned, co-located military facilities might be used for contingency. At off-site locations it is likely that only military ATCCs and/or Air Defence sites would be large enough to provide significant civil ATM capacity.

The issues involved in their use for civil operations are:

- The functionality provided by military ATC Operations and Air Defence systems may be unsuitable for civil operations. e.g. no flight plan processing or flight data presentation;
- The workstations and systems often are, and may be likely to remain, significantly different from those used within civil ACCs. Their use by civil controllers would necessitate an expensive ongoing training commitment;
- Military ATS/Air Defence air/ground and ground/ground communications may not be suitable for civil operations;
- National defence commitment may restrict availability of this resource;
- States will need to ensure positive

replies to these issues in order to use military sites when setting contingency planning requirements with State Authorities.

10.9 OFF-SITE SUPPORT FACILITIES

If States are to rely on support facilities, such as off-line software development systems, for operational continuity, it will be necessary to use as many of the support facilities as possible to provide a reasonable level of operational capacity.

The issues are as follows:

- The various support facilities will have their own workstations and drive systems allowing them to operate independently. To provide an operational service these workstations must be physically and functionally nearly identical to those used for the operational service. This could be achieved by providing all support facilities with operational workstations and systems but this will be costly and results in a complex, fragmented contingency operation;
- The systems' costs and complexity could be minimised by co-locating support functions at one facility and providing it with one set of operational systems onto which all support workstations could be configured for contingency operations;
- In order to provide a safe operational service the support facilities need to have levels of building and system integrity similar to the operational Centres. The use of common systems provides the required operational systems integrity. However, providing the building and plant to the required integrity effectively requires another operational building;
- Another operational building's Support facilities will pose additional problems in meeting a contingency response time of 24 hours and will be heavily dependent on the "operational readiness" of the support systems. At times they will be used for development and evaluation work involving new or modified hardware and considerable time might be required to return them to their 'operational' state. It will then be necessary to certify the support equipment as fit for operational use. This certification time might be significant;
- The support facility will not otherwise require operational communications with aircraft, airports and adjacent Centres. Providing these facilities involves additional expense and raises a number of safety issues which must be resolved;
- The layout of the workstations for the various facilities needs to replicate an operations room which may be unsuitable for the normal support work and may require a larger building;
- The use of support facilities offers a costly and ineffective solution to ATS contingency. It requires a support Centre of operational integrity but one which might not reliably meet contingency response time requirements.

10.10 TOWER (ATC)

Contingency capabilities for ATC tower outage are considerably limited due to the requirement to have an unobstructed view of the manoeuvring area on the airport, as well as the airspace in the vicinity of the aerodrome. Line of sight is particularly important for traffic evolving in the approach and departing area and on the active runway(s). It follows that contingency measures for ATC tower outages should be sought on the airfield itself.

States may wish to keep vacated towers in condition for eventual contingency operations.

The advantage is that remote control and monitoring equipment, ground/ground communication lines for both data and voice are still operationally available.

In the decision/consultation process, attention should be paid to whether or not the following devices can be kept technically in order:

- Approach and landing aids;
- Airport lighting and Surveillance and communication facilities;
- Access to the world-wide AFTN/CIDIN.

Should an airfield not have a vacated tower available, contingency arrangements could be sought in mobile tower facilities which, with cost/benefit aspects in mind, might be used jointly by both civil and military authorities.

A last resort option might be to re-locate the tower to another part of a terminal or other building on the aerodrome where communication facilities can be made available.

APPENDIX D - TEMPLATES TO DEVELOP CONTINGENCY PROCEDURES

Two generic templates are provided to support the development of contingency procedures for Emergency and/or degraded modes of operation:

- for events having a technical cause;
- the other for events having an operational cause;

The purpose of each template is to assist planners in developing detailed technical and operational actions/responses:

- along a "timing" starting with the occurrence of the event;
- making clear the status of the System as a consequence of the actions/responses.

As explained in the Guidelines Step 2.2, only events "altering the normal operations" are considered below.

The part of contingency life cycle of interest is the "normal", "emergency" and "degraded modes". The event may or may not trigger emergency and/or degraded modes of operations. Therefore both contingency modes are considered

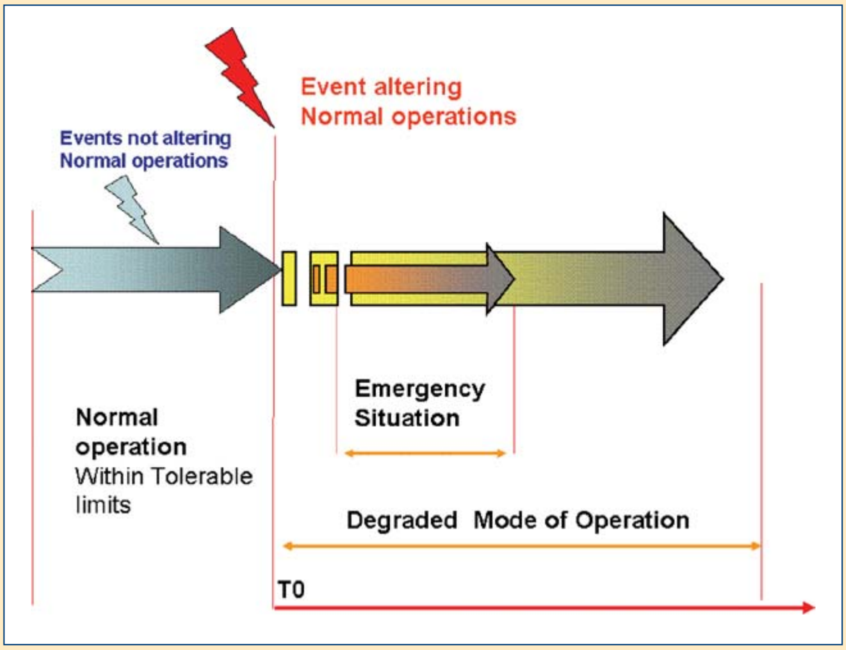


Figure 26: Emergency and Degraded modes part of Life cycle

EVENT WITH A TECHNICAL CAUSE

Time	*Trigger*	*Technical Action to perform after trigger*	*Operational Action to perform after trigger*	*Mode of operation*
T0	Event	Detection of event		Normal
T0 + X (in seconds or minutes)		- Event threshold to activate the Technical degraded mode procedure - Notification to OPS Supervisor	OPS supervisor informed of technical event occurrence	Normal
T0 +Y in minutes	Technical decision of Go/No Go?	Technical Supervisor decides Go/No-go.		
ASSUME "NO GO" DECISION TAKEN : CONTINGENCY PROCEDURES TO BE ACTIVATED				
T0 +Y in minutes			Activation of Operational Emergency/ Degraded mode procedure	Emergency/ Degraded Mode
T0 +Z in minutes			Emergency/ Degraded Mode procedure completed	Emergency/ Degraded Mode

EVENT WITH AN OPERATIONAL CAUSE

Time	*Trigger*	*Technical Action to perform after trigger*	*Operational Action to perform after trigger*	*Mode*
T0	Event	Detection of event		Normal
T0 + X (in seconds or minutes)			- Event threshold to activate the degraded mode procedure - Notification to Tech Supervisor (if needed)	Normal
T0 +Y in seconds minutes	OPS decision on Go/No Go?	Operational Supervisor decides Go/No-go		
ASSUME "NO GO" DECISION TAKEN : CONTINGENCY PROCEDURES TO BE ACTIVATED				
T0 +Y in seconds minutes		Technical Supervisor activates technical part of the emergency/degraded mode procedure (if any).	Activation of Operational emergency / degraded mode procedure	Emergency/ Degraded Mode
T0 +Z in minutes			Emergency/Degraded Mode procedure completed	Emergency/ Degraded Mode

APPENDIX E - EXAMPLE OF APPLICATION OF THE "PLANNING" PROCESS

This example is provided for the sole purpose of illustrating the different steps of the approach proposed in chapter 8.2 Planning Process.

1. INVENTORY OF THE UNITS/SERVICES/FUNCTIONS OF AN ANSP -

The context is an ANSP with a single ACC, an APP co-located with the ACC. In addition, the ANSP provides ATS to a medium size airport. There is no Military ATC provider.

The following services are supplied by external suppliers:

- MET and AIS;
- IT and Power supply.

2. IDENTIFICATION OF "REALISTIC EVENTS" -

From now onwards, we consider the ACC unit. The identification of "realistic events" is conducted as proposed in Step 2.2 Filtering to determine "realistic events".

One of the "realistic event" altering normal operations identified is the total loss of External Power supply (e.g. hazard H-PS_1 of the Building related events in Appendix B- List of Events to Support Risk Assessment.

3. DO I HAVE A PLAN TO MANAGE THE CONSEQUENCES OF THE "REALISTIC EVENTS"?

The design of the "power supply" in the ACC is as described below.

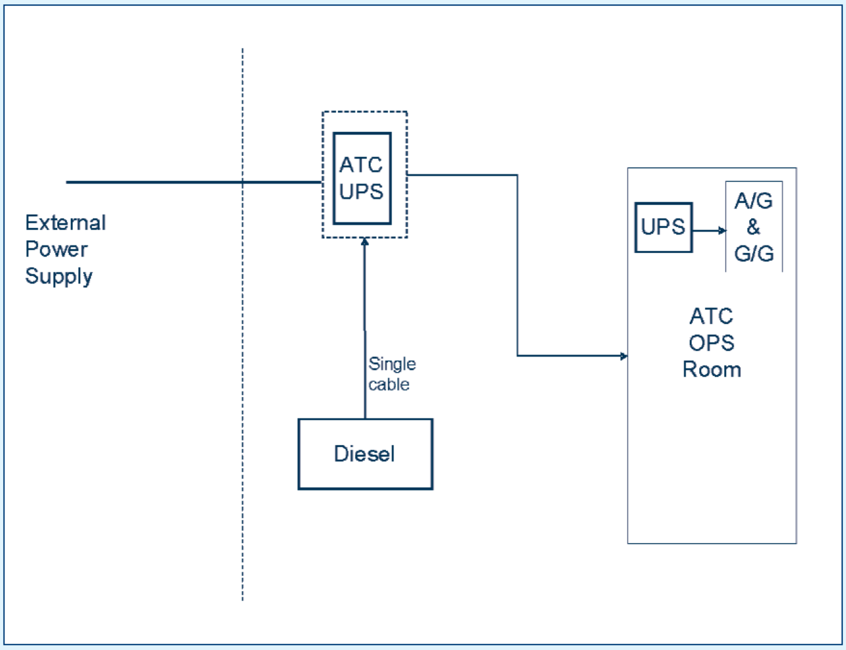


Figure 27: Example of "Power supply" design

To meet the Safety requirements, a ***"Clear the sky procedure"*** exists to deal with such an event. The existing procedure is:

Time	*Trigger*	*Technical Action to perform after trigger*	*Operational Action to perform after trigger*	*Mode*
T0	(Power lost)	Equipment alarm Technicians alerted of loss of power alarm		Normal
T0 +10 minutes	No ATC Diesel generator	- Check why Diesel generator is not functioning? - Call External Power Supplier to see why power is unavailable and when it will come back.		Normal
T0 +20 minutes	Technical Supervisor to take Go/No-go Decision.			
ASSUME "NO GO" DECISION TAKEN: CONTINGENCY PROCEDURES TO BE ACTIVATED				
T0 +20 minutes	Technical Supervisor decides "No Go"	Technical Supervisor decides "No Go". Technicians shut down non-essential equipment	A/G, G/G available. No more departing aircrafts allowed. OPS Supervisor: - inform adjacent centres that the ANSP is closing airspace and releasing traffic early (6 minutes) - inform adjacent centres not to send aircrafts to FIR	Close down mode
T0 +30 minutes	Applying vertical separation		Orderly clearance of FIR Inform CFMU Issue NOTAMs	Close down mode
T0 + 40 minutes	FIR closed		Inform management.	Closed

3.1.DO THE MEASURES MEET THE REQUIREMENTS OF THE POLICY?

3.1.1. EMERGENCY/ DEGRADED MODES OF OPERATION

In this context, the first verification is to ensure that the "Safety" requirements (i.e. Fail to Safe) are effectively met.

The ANSP reviews its existing procedure. After analysis, it is found that the previously existing procedure is built on the erroneous assumption that Power would be available in the ATC OPS room for 20minutes (Go/No Go decision) + 20minutes ("Clear the sky") for the whole set of equipment (ODS, FDM, A/G, G/G) .

This assumption is erroneous as UPS supplies only 20 minutes of power to ATC room. Therefore, a new procedure is developed to ensure a proper management of the event.

Two actions are then taken:

1. Improve the "resilience" of the System by:
   - 1.1. Adding additional UPS to ensure the availability of A/G and G/G communications;
   - 1.2. Adding additional UPS to increase the duration and reliability of the back-up;
   - 1.3. Double the cable between the Diesel generator and the UPS.
2. Re-design the "Clear the sky procedure" as follows

Time	*Trigger*	*Technical Action to perform after trigger*	*Operational Action to perform after trigger*	*Mode*
T0	(Power lost)	Equipment alarm Technicians alerted to loss of power alarm		Normal
T0 + 30 seconds	No ATC Diesel generator	- Check why Diesel generator is not functioning? - Call Power Supplier to see why power unavailable and when it will come back.		Normal
T0 + 2 minutes	Tech Inform Ops,	Technician: - inform Ops - inform Tech management of power loss. - continue to start ATC Generator	OPS: - compile list (3 minutes), - inform management that airspace may need to be closed - get extra ATCO to compile list	Normal
T0 +7 minutes	Technical Supervisor to take Go/No-go Decision.			

ASSUME "NO GO" DECISION TAKEN : CONTINGENCY PROCEDURES TO BE ACTIVATED

[7] A/G: Air-Ground Communications; FDM: Flight Data Management

Time	***Trigger***	***Technical Action to perform after trigger***	***Operational Action to perform after trigger***	***Mode***
T0 +7 minutes	Technical Supervisor decides "No Go"	Technicians shut down non-essential equipment	A/G,G/G available. No more departing aircrafts allowed. OPS Supervisor: - inform adjacent centres that this ANSP shall be closing airspace and releasing traffic early (6 minutes) - inform adjacent centres not to send aircrafts to FIR - apply vertical separation. ***OPS supervisor informs management of No Go*** (No decision is required from management to close down airspace as the procedure has been signed off)	Close down mode
T0 +10 minutes	Radar Service terminated (after applying vertical separation)		Orderly clearance of FIR Close FIR Inform CFMU Issue NOTAMs	Close down mode (procedural)
T0 +20 minutes	Loss of surveillance and FDM	Main A/G communications still available (additional UPS) G/G communications still available (additional UPS)	Main A/G communications still available (additional UPS) G/G communications still available (additional UPS) Use of paper list of flight data	Close down mode (procedural)
T0 + 27 minutes	FIR closed		Inform management.	Closed

3.1.2. "SERVICE CONTINUITY" MODE OF OPERATION

Once solved the issue of "Emergency/Degraded modes of operation". The question of "Service Continuity" is to be addressed.

The approach proposed in Step 4.2 Develop or change contingency measures for "Service Continuity" might be followed.

1) Impact assessment of the loss or disruption of Service

The services impacted by the "loss of power" are the Air Traffic Services (and other ANS co-located in the same OPS room) provided by the ACC.

For instance, at the policy stage, it may have been agreed with the Airspace users (e.g. main national airline) and the national airport that an interruption of ATS longer than 6 hours is not tolerable in summer time (tourism activities). As no other constraints lead to shorter "maximum agreed period of disruption", the MAPD of the service is 6 hours.

2) Is there a potential need for "Service Continuity"?

a) Is there a potential need for "Service Continuity" based on event

Considering the event "Loss of power supply" the likelihood to have a loss of external power supply longer than 6 hours is to be discussed with the Power supplier. A requirement to have power restored in a shortest period should be included in the service level agreement with the supplier.

Therefore on the sole ground of the "power supply" event it might be not necessary to develop ***"Service Continuity"*** measures.

b) Is there a potential need for "Service Continuity" based on MAPD

However, "power supply" is only one event and it is very likely that other types of events may lead to longer disruption of services. Thus, for a MAPD shorter than 48 hours, there is a potential need for Service continuity and it is recommended to investigate further possible "service continuity" strategies.

3) Determining and developing "Service Continuity" strategies

On the basis of the guidance provided in Appendix C - ANS Contingency Strategies, possible service continuity strategies are:

- Either moving personnel to locations within the State:
  - TMA/APP is a possibility; ATS Training/ development unit/ Simulator is also a possibility if such a facility exists.
  - other ACC is excluded (there is only a single existing national ACC);
  - consider building and operating a specific "contingency centre": the economical viability of this option should be assessed and the option be abandoned if not economically viable;
  - military units (ATS and/or Air defence) do not exist;
- Or moving personnel to locations within adjacent State(s): other ACC or other TMA.

4) Economic Assessment

The economic viability of the remaining strategies is to be assessed:

- Equipment of TMA and APP to ensure part of the ACC capacity during Service continuity;
- Equipment of ATS Training/ development unit/ Simulator to fit operational use...
- Use of adjacent centre spare capabilities: the arrangements should be clearly established (LOAs) along with the financial aspects (costs of services, mutual aid);
- Building and operating a specific "contingency centre": it is likely that in this context of an ANSP with a single ACC, this option is not viable.

If no viable Service continuity solution can be drawn, the requirements in terms of capacity (traffic handled) should be revisited in consultation with the airspace users and the airport.

5) Safety Assessment

All contingency procedures (Emergency, degraded modes and Service continuity) should be assessed in terms of Safety.

6) Document the procedures

All contingency procedures (Emergency, Degraded modes and Service continuity) should be documented.

APPENDIX F - CHECK LIST OF PROVISIONS TO INCLUDE IN CONTINGENCY AGREEMENT BETWEEN ANSPS

A standard contingency agreement should contain at least the following elements:

- Name of the Parties , and of their duly mandated representatives
- Scope of the Agreement, identification of the services concerned
- Provisions on financial aspects, if any
- Identification of the decision taking role/body in both failing and aiding units, also in respect to the declaration of the contingency phases
- Applicable operational procedures and / or national regulations
- Identification of the geographical area and level range for which the contingency service is provided
- Identification of the types of flights for which the contingency service is provided
- Procedure for the transfer of control
- Radio-telephony procedures
- Criteria for the use of the CFLAS by the failing and the aiding units
- Restore [end of contingency] procedures
- ATFM/AIS measures
- Identification of the logistic and operational infrastructures/facilities intended to be used or managed by the relocated staff
- Administrative / security procedures for the relocated staff
- Contact points for the relocated staff
- Compliance with Article 10.2 and 10.3 of Regulation (EC) No 550/2004 (notifications and approval)
- Oversight and supervision
- Allocation of liabilities
- Dispute settlement
- Entry into force, duration and termination

APPENDIX G - SYSTEMS ENGINEERING PERSPECTIVE ON CONTINGENCY STRATEGIES

1. GENERAL

The broad operational, managerial and organisational actions associated with each contingency strategy are detailed in Appendix C - ANS Contingency Strategies. ***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.

2. DIFFERENT ENGINEERING APPROACHES

The main Engineering support approaches identified are:

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

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.

2.1 '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.
- Communications are supported between systems and operational staff because they are both employed by the same organisation.

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, and pandemics).
- Key engineering staff may be required both to identify the causes of contingency and also to activate a fallback facility leading to staff shortages.

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.

2.2 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).
- Contractual agreements are necessary to explicitly state the extent of support that may be expected by an ANSP from a contractor under contingency.
  - *Liaison with Contractors and sub-Contractors is necessary during the planning phase.*

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 breeches in security.
- Contractors may not be familiar with all aspects of an ANSP's Safety Management System and may have very different views of safety culture both before and during contingency. This problem can be exacerbated when primary contractors employ a range of additional sub-contractors that have only an indirect relationship with the ANPS.
- Communications overheads may increase as ANSP management have to deal with contingency and also organise necessary support from external contractors.
- In some smaller ECAC states, there may be a monopoly on infrastructure provision - especially in communications. These companies may be unwilling to meet service levels expected by ANSPs under contingency. State monopolies may also lack the technical resources to provide levels of reliability and support anticipated by ANSPs.

MITIGATION ACTIONS

- 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). These documents must consider the guaranteed number of staff and the length of time that an ANSP may call upon from a contractor under contingency.
- Such agreements should state the 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 and plan for communication problems that might otherwise delay an effective response to any future incident.
  - *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 breeches 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.
- Deploy monitoring systems, for example in Local Area Networks, to help diagnose the source of complex system failures that may stem from complex interactions between 'in house' applications and systems maintained by subcontractors.
- Steps can be taken to ensure that sub-contracting staff are integrated within the ANSP's Safety Management Systems before contingency.
  - *In smaller states, ANSPs must work with monopoly suppliers - with support from the NSA to achieve the highest levels of assurance possible for contingency provision before an adverse event occurs. Validation measures should be in place to ensure that, for example, national telecoms companies can meet ANSPs requirements and that they understand the critical nature of the services that they provide to ATM operators.*

2.3 'COMMERCIAL OFF THE SHELF' (COTS) APPROACHES

More and more CNS/ATM systems include COTS elements. This trend is likely to 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.*
- Problems can arise from complex interactions between COTS components and other bespoke elements of the ATM infrastructure.
  - *e.g. It can be difficult to diagnose intermittent failures that stem from COTS systems if ANSPs cannot look inside those components to identify the sub-systems that are failing.*

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.*
- These problems can be exacerbated with COTS components have been installed by sub-contractors who themselves do not have direct access to the engineering details of the systems that they have provided.
- During crisis/contingency, there is often a pressing need to contact vendors 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.*
  - *The original vendors may not be aware that their application is being used in a particular configuration within an ANSP's infrastructure and so may only be able to offer limited support.*

Smaller ECAC states may lack the 'market power' to obtain urgent support from suppliers in the immediate aftermath of a contingency.

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? Week-end?)*
  - *Which stock of back-up supplies?*
  - *Participate in vendor's reporting and update schemes to ensure that the ANSP can learn from any previously reported incidents.*
  - *Deploy monitoring systems, for example in Local Area Networks, to help diagnose the source of complex system failures that may stem from COTS applications.*

2.4 TECHNICAL 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.
  - *Within the context of SES, several ANSPs have begun to develop agreements for the joint procurement of common infrastructures, these agreements provide a template for the exchange of technical support under contingency,*
- 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), the 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.
  - *There are few examples of engineering staff being deployed to help an ANSP from another ECAC state, in time to respond effectively to a contingency, Hence this approach remains largely unproven even if the situation may change with the increasing use of common infrastructure components under SESAR.*
- It is important not to underestimate the communications problems that can arise between employees from different ANSP's, these extend beyond the procedural differences that affect technical operations and include different attitudes to many aspects of Safety Management.
  - *There is a risk that the exchange of systems staff under contingency may introduce more risks than it resolves, as those individuals may not fully understand the detailed engineering of another ANSP's infrastructure.*
- *There is a danger in smaller ECAC states that informal working practices will emerge to develop effective responses to contingency with neighbouring states. However, these practices may eventually be very different from those measures that are 'officially' sanctioned in LoAs.*

MITIGATION ACTIONS

During Planning phase:

- Address as required the legal status, competency and certification of support engineers provided by other countries.
- Technical and engineering exchanges should be conducted before a contingency occurs so that staff become familiar with the environment and SMS procedures in a neighbouring state well before a contingency takes place.
- 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, insurance, 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.

Many of the mitigations for sub-contractors also apply here given that the employees of another ANSP will meet the same communications issues that complicate the role of external agencies under contingency.

2.5 CROSS BORDER INFRASTRUCTURE COOPERATION

Several ECAC states rely on their neighbours for critical elements of their infrastructure provision - for example, geography may dictate that ANSPs have to use radar and communications systems from other states in order to maintain levels of service across High Seas areas where they cannot otherwise provide CNS functions.

MAIN CHARACTERISTICS
● Geographic and technical constraints on smaller ECAC states can result in some ANSPs relying on their neighbours for systems engineering support - for instance if a service provider has no available land mass on the periphery of an High Seas FIR they may request data from a neighbours radar site that does cover elements of their air space.
POTENTIAL RISKS FOR CONTINGENCY
● This creates two issues for contingency - how to ensure that the loss of these services from neighbouring ANSPs does not trigger contingency and also to ensure that such services can be maintained under contingency when technical staff from other states may be needed to reroute CNS feeds. ● Changes in the infrastructure of the state hosting remote services may disrupt the flow of CNS data between neighbouring states and this can trigger a contingency. ● Routine maintenance and upgrades on remote infrastructure are not under the control of the ANSP that shares these services. This can exacerbate existing problems - for instance, forcing the ANSP to use procedural control techniques.
MITIGATION ACTIONS
During the design and implementation of contingency provision, ANSPs can increase the resilience of CNS feeds with neighbouring states - for example by using satellite links that are less vulnerable to the breakages that can affect marine data cables or by creating multiple cables to ensure redundancy in transmissions between states, Staff may have to be trained on appropriate procedures that can be called upon when remote infrastructure elements are lost. Systems engineering teams must be given effective communications support so that they can quickly contact their colleagues in the neighbouring ANSP should remote CNS data flows be interrupted.

3. A LIFECYCLE APPROACH TO SYSTEMS ENGINEERING IN CONTINGENCY.

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

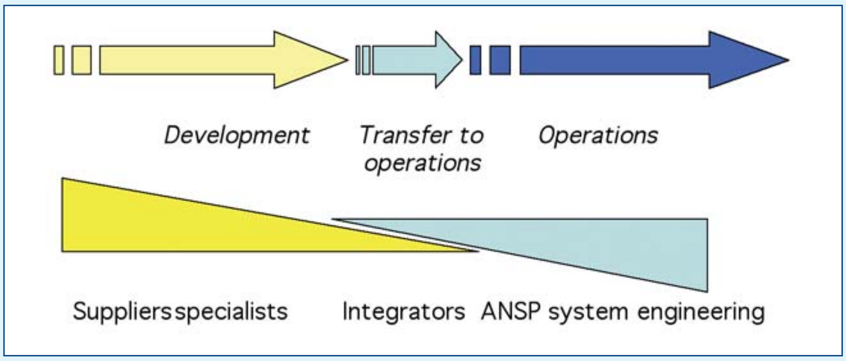


Figure 28: Suppliers and ANSP Engineering staff vis a vis ATM Life Cycle

As illustrated above:

- 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. Or the original supplier may maintain responsibility for looking after the system - if this occurs then the people who originally developed the application are usually replaced by a smaller number of support technicians who are often available 'on call' to an ANSP.
- Particular concerns arise in smaller ANSPs where there may not be the same 'defences in depth' that are provided in larger states. Similarly, there may not be the same range of internal technical support to 'cope' when suppliers hand-over equipment if subsequent problems arise.

As changes are introduced to the initial system:

- The external supplier may lose the necessary contact with the system as it evolves.

  This may reduce their ability to be of immediate assistance during any subsequent contingency.
- Even if a supplier continues to provide on-site support, the original development teams may be replaced by technical staff who do not understand the detailed underlying engineering of an application that may be necessary under a potential 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.
- The impact of changes in support to systems infrastructure on contingency planning should be considered within the wider forms of risk assessment that are conducted before new applications are handed over to an ANSP.

3.1 THE IMPACT OF DIFFERENT FAILURE MODES ON CONTINGENCY

A number of different failure modes can lead to contingency. It is unlikely that all subsystems within any major centre will totally fail at the same time given that considerable efforts have been made to remove single points of failure. However, there are differences in partial failure modes that complicate the response to contingency:

- Intermittent failures. A fault may appear, for example within CNS applications, that occurs for a short period of time and then 'resolves' itself before engineering staff can identify the cause. This may occur when periodic faults affect hardware components. However, unless the cause is identified there is a considerable danger that a worse contingency may occur if the fault returns. ANSPs should work with contractors to deploy sufficient monitoring resources to diagnose the cause of intermittent failures.

- Partial Loss of Sub-systems. It can be difficult to identify the precise causes of failure when only a small number of systems seem to be affected. Faults can arise from the interaction of applications provided by several different engineering groups within an ANSP or from different suppliers. This creates considerable problems in identifying who is required to respond to a contingency situation.

This list is a brief summary of failure modes that have been observed in ECAC states, ANSPs should assess the impact of other potential scenarios upon their operations.

3.2 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.

APPENDIX H - PRINCIPLES FOR THE CONTINGENCY PLAN ECONOMIC ASSESSMENT

1. INTRODUCTION

This Appendix presents some high-level principles for conducting an economic assessment of Contingency Plans (CP) for Service Continuity.

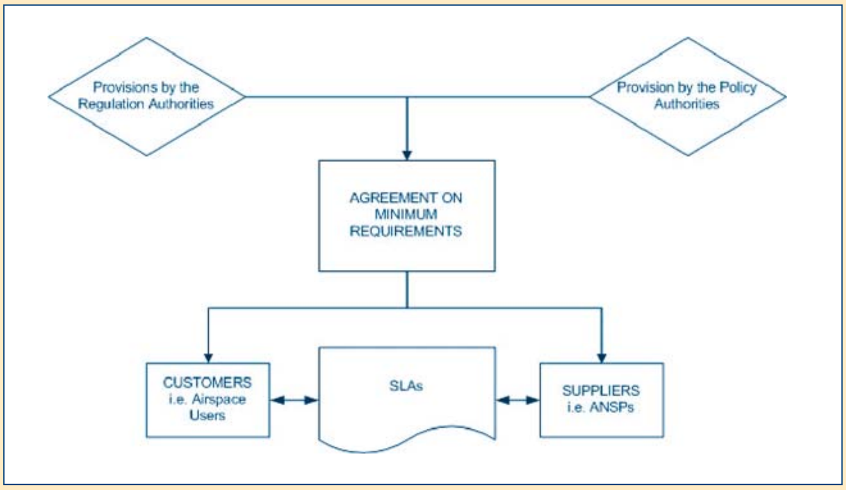
Other types of contingency plans for "Emergency/degraded modes of operations" are driven by safety/security considerations. They describe measures to be taken immediately after an outage occurs and to be maintained for a reasonably short time thereafter. As such since they are driven by safety and security considerations they should not be assessed on economic grounds.

The guidance provided in this Appendix does not sit in isolation and should be read, understood and acted upon as necessary, in the context of the other sections of the Guidelines most notably the Policy and Planning sections .

As part of the process of planning contingency measures, State authority/ policy making authority, ANSPs and their customers (Airspace users and Airports) should put in place a process to set or to come to an agreement as to the requirements to be met by the CP for service continuity. Details on this process are given in section Policy of the Guidelines.

At the end of this process, several sets of requirements might be established:

- ***Safety and security requirements.*** These requirements would be defined primarily by the regulatory and policy-making authorities in consultation with ANSPs and should ***not be traded-off at the expense of increases in Capacity and/or Flight Efficiency.*** These requirements would be defined primarily by the regulatory and policy-making authorities in consultation with ANSPs.
- ***Capacity and Flight efficiency requirements***. These requirements for Capacity and Flight efficiency provided by an ANSP at different times after outage would be defined further to consultations between all interested parties including ANSPs Airspace Users, Airports and bodies capable of expressing the general interest of the travelling public and of society as a whole. These provisions can be captured in appropriate bilateral or multilateral Contingency Service Level Agreements [SLAs] negotiated between the relevant parties.


Provisions by the Regulation Authorities
Provision by the Policy Authorities
AGREEMENT ON MINIMUM REQUIREMENTS
CUSTOMERS i.e. Airspace Users
SLAs
SUPPLIERS i.e. ANSPs

2. CHALLENGES IN ECONOMICALLY ASSESSING CONTINGENCY PLANS FOR SERVICE CONTINUITY

In order to help decision makers and contingency planners to scope Contingency Plans for Service Continuity with a higher degree of confidence, the plans should be substantiated by economic assessment before stakeholders' money is committed and work towards implementation begins.

Contingency is an inherently unlikely event. Therefore economic assessment of Contingency Plans for Service Continuity raises specific issues:

- A prime objective is to achieve adequate contingency capability at a reasonably acceptable cost.
- Assessment of the value needs to take account of the very small likelihood of events such as fires and also the financial impact of such events on the ATM provision.

The role of Economic Assessment is to provide a means of assessing how to meet that strategy in the most cost effective way.

The economic assessment of Service Continuity aims to obtain systematic, qualitative and/or quantitative inputs for the decision-making process by assessing the merits of candidate mitigating strategies, subject always to safety and security requirements and within the context of legal national, European (SES) and international (ICAO) obligations, budgetary constraints, priorities and opportunities.

3. CHARACTERISTICS OF CONTINGENCY PLANS FOR SERVICE CONTINUITY

3.1 DRIVING FACTORS

Whilst the driving factors behind contingency planning for "Emergency/degraded modes of operations" are safety and security, the driver for Contingency Plans for Service Continuity is economics: minimising the losses and costs that would occur in case of occurrence of a major outage if no mitigating measures would have been adopted and be in place.

Reduced losses and costs are, as the case may be:

- reduced losses of revenues (e.g. en-route and TMA charges, airport charges and airport ancillary revenues, taxes)
- reduced operating costs (extra fuel, insurance, staff overtime, compensations due as a result of commercial policies or law -such as EU's passengers rights policy-)
- reduced losses for the customers of the airspace users (e.g. passengers, mail and cargo)
- reduced losses for the local, regional or European economy

Economic factors such as the loss of revenues, penalties and increased insurance premiums form part of the Impact Assessment discussed in Planning Step 4.2.

The economic analysis measures the benefits of having service continuity in place, from the perspective of the various stakeholders: airspace users, ANSPs, airports, passengers and the society (where possible to assess).

Such benefits are a direct function of:

- duration of the outage,
- pattern of capacity recovery and
- reaction of neighbouring ATM units to the possible chaos created by the outage.

The objective of economic assessment of Service Continuity is to seek to identify the capacity that each mitigating strategy could achieve and at which cost. In a perfect world the optimum level of service [intended as accommodated demand] for each contingency phase should be chosen so that its marginal cost for any extra service unit is lower, or at most equal to, the corresponding loss.

3.2 OBJECTIVE OF THE ECONOMIC ASSESSMENT

The objective leading to Contingency Plans for Service Continuity is to ensure the minimum impact of disruptions in addition to satisfying the safety and security requirements. Disruptions can be classified: flight cancellations; flight re-routings to non closed airports; extra flying time due to re-routings around the Area of Responsibility (AoR) of the failing unit; and extra minutes of delay on the ground.

4. ECONOMIC APPRAISAL GUIDELINES

Purpose: assist ANSPs and regulators in assessing the rationale of investing in Contingency planning for Service Continuity and in securing (best possible) value for money.

Method: a list of high level guidelines based on the evidence gathered and the conclusions drawn from the performance

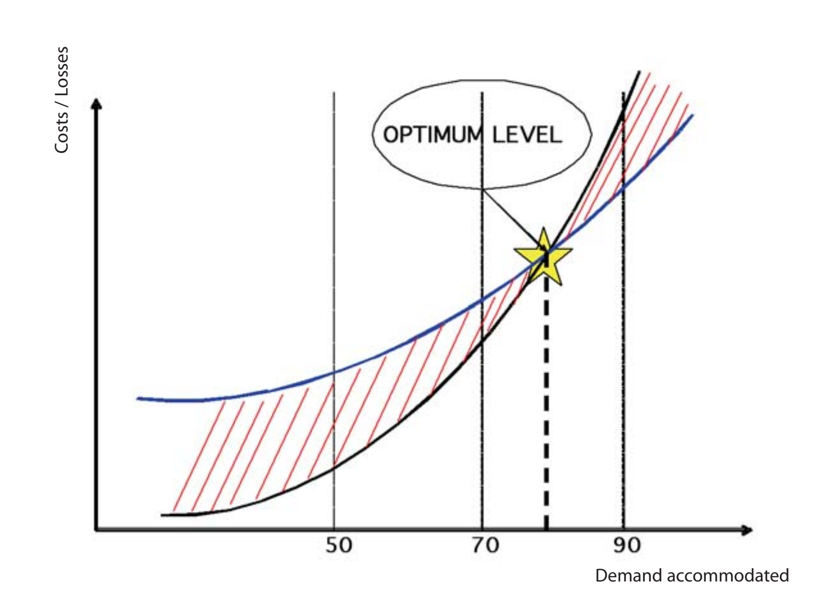


Figure 29 - Optimum contingency level of service [accommodated demand]

of an economic assessment of different possible contingency strategies performed in different kinds of environments.

The key steps of a logical framework of the economic assessment could be as follows and are summarised thereafter.

As indicated in the conclusions no decision to invest depends solely on the results of an economic assessment of candidate strategies Economic Guidelines rather insist that the economic analysis is only a part of the decision making process in Service Continuity.

Such guidelines include:

4.1 IDENTIFICATION OF THE MAIN CATEGORIES OF OUTAGES

A variety of situations may result from disruptions requiring Contingency Planning. They range from:

- Routine situations (e.g. partial loss of radar coverage, unavailability of ODS) where disruptions would partially affect ANSPs during short periods of time (ranging from some hours to a few days).
- Infrequent situations (e.g. major software bug, floods, earthquakes, terrorist attacks, pandemics, where complete ATM Units and or operational/technical staff would be totally out of service for long periods of time (the time required to fix the bug, rebuild the facility and / or to recruit & train the staff to the required level).

The cases of extreme disruptions cannot be dealt with in the same way as incidents which are part of the usual life of any ATM unit. Their severity justifies the development of Contingency Planning for Service Continuity.

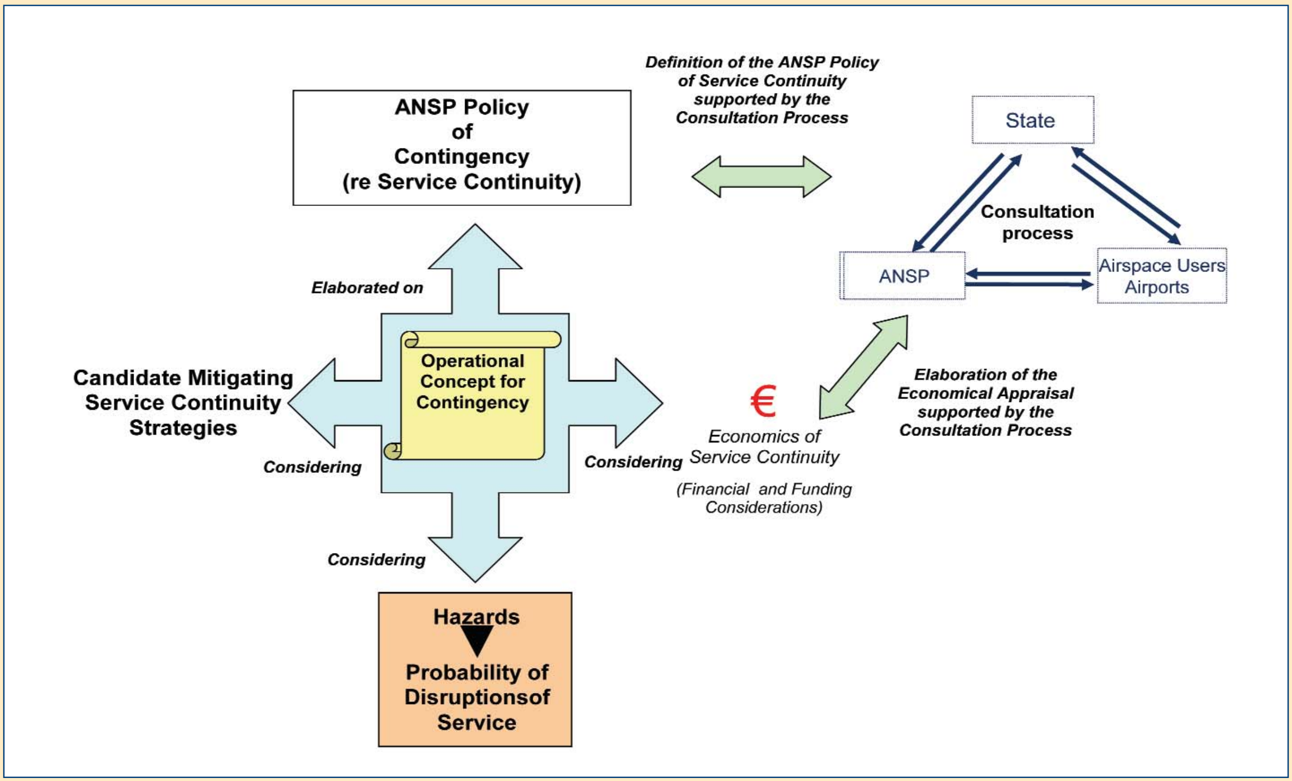

Definition of the ANSP Policy of Service Continuity supported by the Consultation Process
ANSP Policy of Contingency (re Service Continuity)
State
Consultation process
ANSP
Airspace Users Airports
Elaborated on
Operational Concept for Contingency
Candidate Mitigating Service Continuity Strategies
Considering
Considering
Considering
€
Economics of Service Continuity
(Financial and Funding Considerations)
Elaboration of the Economical Appraisal supported by the Consultation Process
Hazards
Probability of Disruptionsof Service

Figure 30 - a view of a process

4.1.1 OPERATIONAL IMPACT OF SEVERE DISRUPTIONS

For the purpose of performing an economic assessment this second category of severe situations should be split into similar sub-categories:

- A facility is out of service but the staff is operational (flood, explosion at a moment when there is almost no staff present) - see description under Appendix C - ANS Contingency Strategies of Guidelines
- A major software bug has occurred - see description under Appendix I-Special Cases §1.4 of Guidelines
- A facility is operational but part of the staff was hit (pandemics, explosion when staff is present) - see concerning pandemics description at Appendix I- Special Cases, section 3.

The economic assessment is critically dependant on the categories of outages which the ANSP decides (or is bound to) be protected against:

- The cost of the mitigating measures differs from one category of events to another: protecting against destruction of facilities or the failure of hardware mainly requires investment whereas protecting against staff outage requires hiring and training staff from school or external centres.
- The probability of disruptions -hence the cost effectiveness of the mitigating measures- (including the probability that disruptions take place concurrently in more than one single ATM Unit - cases of common failure modes-) differs from one category of events to another.
- The expected duration of the outage -hence the resulting losses- will be different: a software bug will take an unknown number of days or weeks to fix; rebuilding an ACC will take several years (e.g.3 years); hiring, and training staff to the required standard is likely to be even more time demanding.

4.1.2 CATEGORIES OF OUTAGES

Two categories of outages are relevant:

- Outages due to external events
- Outages due to ATM related events

The first category encompasses the events for which the probability of an outage is most remote yet at the same time the economic consequences are likely to be much more severe. Protection against external events has not been top on the priority list of the ANSPs and regulators, whilst ANSPs have already put together safety plans and contingency measures against failures of the ATM system.

Major categories of external events are (list not exhaustive):

- fire,
- extreme object collision (aircraft, meteorite),
- extreme weather conditions (flooding, tornado, lightning),
- earthquakes
- pollution (chemical or else)
- pandemics
- major software bugs
- hostile attacks (terrorism)

ATM related events:

- Contingency Guidelines (Appendix B-List of Events to Support Risk Assessment) give a fairly detailed list of ATM related events in support of the assessment of such internal events.
- For some of them (fire, hostile attacks) defensive barriers are usually built into the ATC system and most ANSPs would challenge the view that e.g. a fire could completely destroy a unit. However such a possibility should not be totally disregarded and ANSPs usually buy insurance to protect against such events.

4.2 ASSESSMENT OF THE PROBABILITY OF OCCURRENCE OF THE OUTAGES

An Economic Analysis (refer below section 11 Error! Reference source not found. as an example) has demonstrated that the probability of occurrence of a major outage is a critical component of the economic effectiveness of Contingency Planning for Service Continuity.

This is because the probability of occurrence (and to a lesser extent the discount rate applied to the cash flows) has a decisive influence on the economic value of an investment:

Example:

A benefit of: ***1 million*** any time (but only once) over 40 years, values ***250 000 NOW*** at a discount rate of 10%

[8] Under the Guidelines this example would fall under the category of events leading to "Degraded Mode of Operation" for a period of time lower than the Maximum Acceptable Period of Disruption ("MAPD"). As such they would not be addressed in an economic analyse exercise focused on Service Continuity

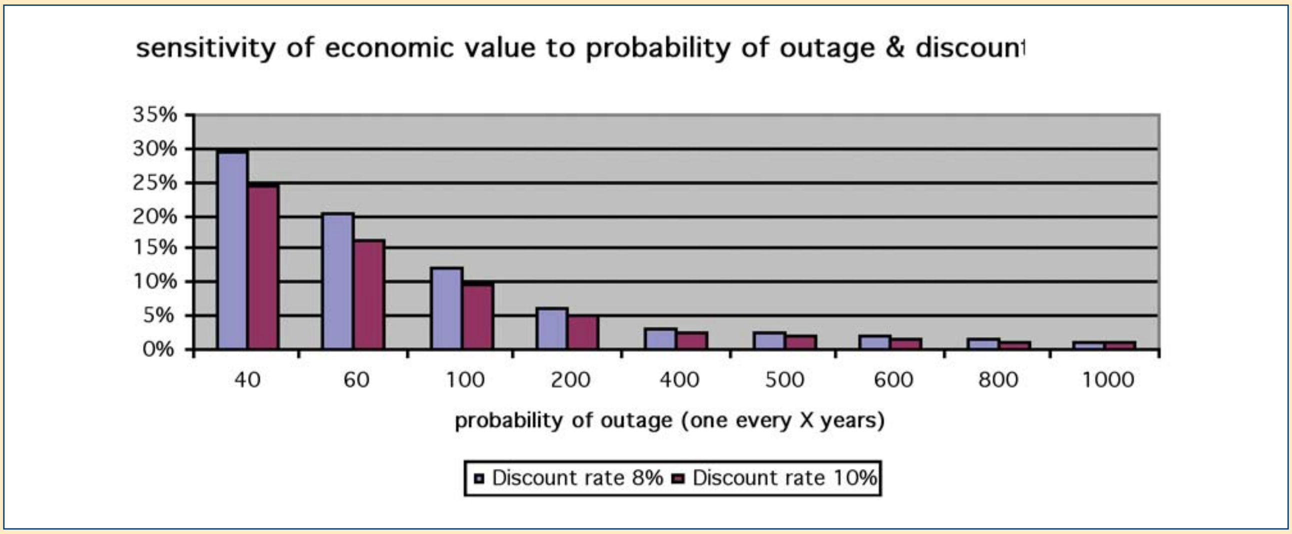


Figure 31 - sensitivity of economic value to probability of outage and discount rate

4.2.1 PROBABILITY OF OCCURRENCE OF THE OUTAGES

The probability of occurrence of each and every outage cannot be a single figure for Europe. The probability of, for example, flooding or an earthquake is very much dependant on local conditions. Not all risk experts would recognise a probability of flooding of once every 150 years as was proposed in the UK after major flooding occurred in summer 2007. It is therefore critical to perform a critical survey and review of all the sorts of outages that could potentially result in a long term outage of an ATM unit.

Whilst ANSPs are best placed to assess the risk of occurrence of an ATM outage, they may require the support of external risks experts to assess the probability of occurrence for each case of external event and each candidate ATM unit.

The external expert will also establish where events are likely to be interdependent and if possible the combined probability of independent forms of outages.

Possibly few experts would release single figures for the probability of an outage. Typically experts would argue that statistics are missing (hostile action) or are questionable (numbers of floods would increase as a consequence of climate change). In such a case they might feel more comfortable with the provision of a range of values.

The intention should be to be in a position to produce and approve a matrix for each ATM unit:

Event	Background description	Probability	Min-Max
Earthquake			
Flooding			
Lightning			
-			
-			
Software Bug			

Figure 32 - Outages likely to affect ATM unit X

When, based on local conditions, experts would conclude that an event is unlikely to occur at a given place, this should be clearly recorded with a probability 0. When the decision is proposed locally not to consider an event, this should equally be justified (on technical, legal or economic grounds) and recorded.

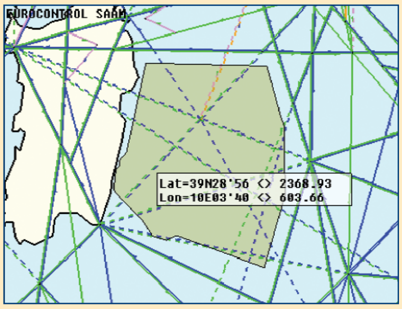
Step 2 of Chapter 8 - Contingency Planning Process could be used to identify and filter the events so as to determine the "realistic events" to take into account in the economic assessment.

4.3 DESCRIPTION OF THE CONSEQUENCES OF THE OUTAGES ("WAIT AND SEE" SCENARIO)

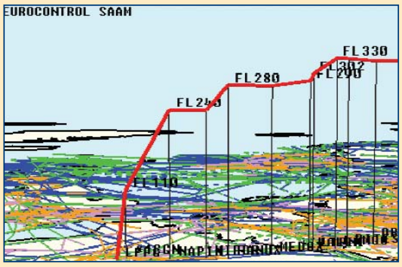
For each ATM unit under their responsibility ANSPs should thereafter describe the practical consequences of each of such events in case No plan for Service Continuity would have been developed and be in place ("Wait and See scenario"):

- Which operational capabilities would be affected
- Which impact on the traffic, take offs, landings etc.
- How long it would take to restore capacity/service provision and the pattern of capacity recovery
- How the neighbouring ANSPs could adapt their capacity/service provision as a reaction to the outage
- The costs.

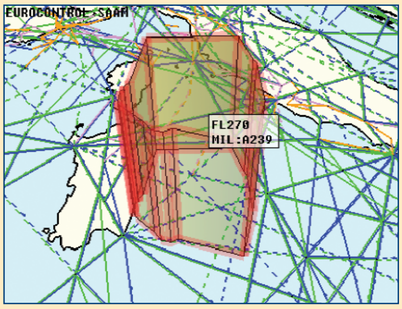
In order to measure the impact on the traffic where no contingency plan for Service Continuity exists, ANSPs could use a tool (e.g. the EUROCONTROL SAAM tool) in support of experts' judgment.



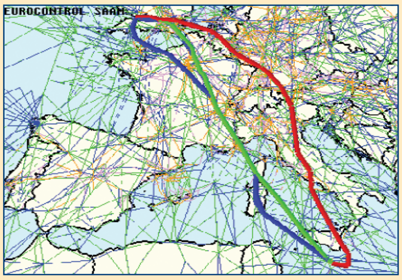
2D network edition



Profile Constraints



3D sectors edtion



Routing Constraints

Measuring the consequences in terms of costs would require the use of an Economical assessment tool (e.g. the EUROCONTROL EMOSIA version customized for Contingency).

The intention should be to be in a position to produce and approve a matrix for each ATM unit:

Event[9]	Operational Capabilities affected	Duration of outage and pattern of capacity recovery	Impact on neighbouring ATM units	Cost of reactive actions
Earthquake				
Flooding				
Lightning				
-				
-				
Software Bug				

Figure 33 - Consequences of Outages likely to affect unit X in "Wait and See scenario"

4.3.1OPERATIONAL CAPABILITIES AFFECTED

The Economic Analysis shows that the outcome is significantly different depending on the portion of airspace affected by the outage. The consequence of closure of En-route airspace is mainly a combination of delays and re-routings:

By contrast, the closure of a TMA triggers flight cancellations. It will also have a major impact on the global system, including local and regional business around the airport and tourism.

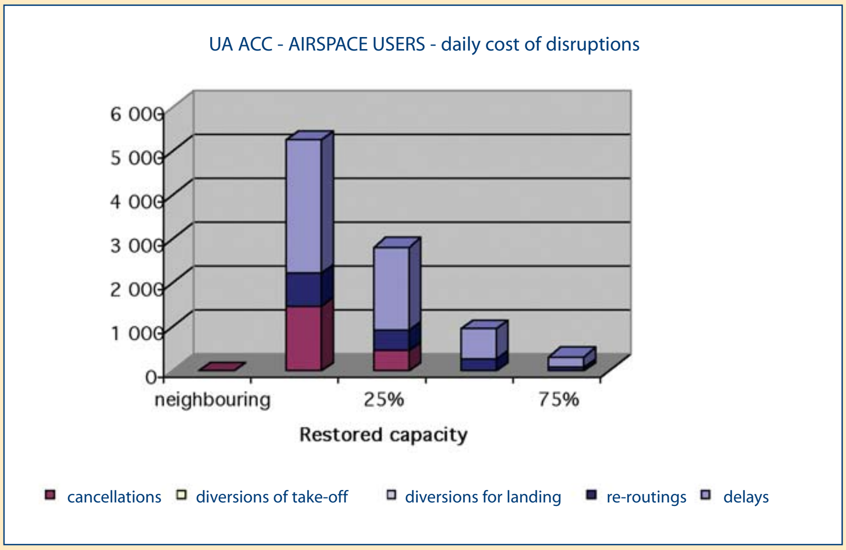


Figure 34 - Airspace users -daily costs of disruptions - En route

The following chart shows the impact on airspace users of a disruption of a unit controlling both en-route and TMA: the cost of diversions represent more than 50% of the total cost for the Airspace Users. The proportion will be even larger when the impact on airports and local economy is taken into account:

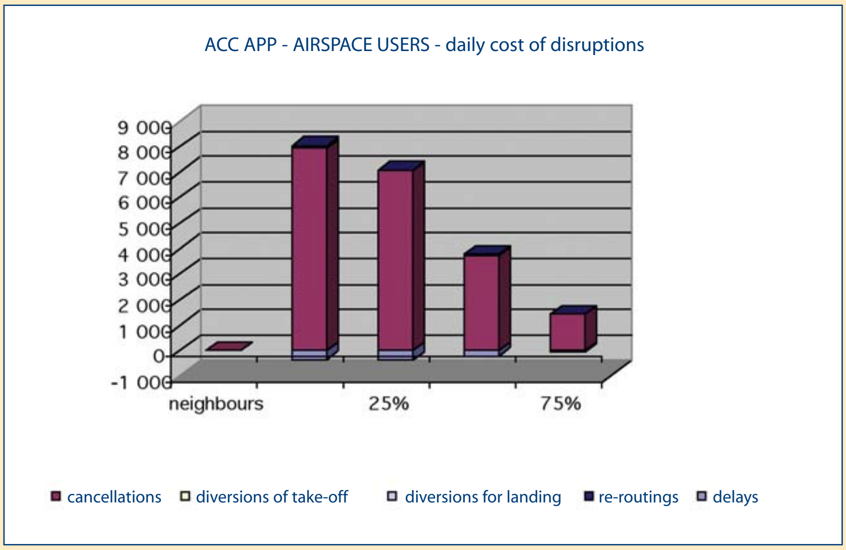


Figure 35 - Airspace users -daily costs of disruptions - En route & TMA

The analysis should describe which ATM services would be hit and how, in particular if and to what extent the En-route, TMA and / or airport traffic would be affected.

[9] Contingency Guidelines Appendix B could form the basis for such categorisation of the events.

4.3.2 DURATION OF THE OUTAGE

Economic impact of such outages is not just a function of the probability of occurrence of an outage but is also a function of the total period of time during which capacity/service provision would be limited or unavailable.

As part of the discussions about the 'Wait and see scenario" the ANSP should define how long it will then take to restore a sustainable ATM Unit capability. Such duration will to some extent be a function of the causing event: possibly, restoring capacity after floods would not take as long as restoring capacity after a fire if the Ops room was protected.

It is not easy to figure out what the pattern of capacity restoration could be. This information is necessary for the successful design and implementation of the contingency plan: at least the duration of the first steps of capacity/service level restoration (expressed in weeks or months) has a significant impact on the economics of the contingency planning.

Such a reasonably descriptive baseline scenario is required to open the dialogue with the Users on solid grounds, which is of vital importance for the quality of the economic assessment and final buy-in.

4.3.3 ACTION BY NEIGHBOURING ANSPS

As soon as an ACC declares a severe outage some of the neighbouring ATM units may need to consider reducing their capacity (e.g. for En-route ACC failure);

The reasons of the neighbouring ATM units to reduce capacity would be:

- Safety reasons, particularly in situations where significant changes in flight profiles would be introduced;
- Familiarisation: controllers would need to form a mental picture of the new environment.

The percentage of any capacity reduction would not be a single figure across Europe. It would on the contrary be heavily dependant on the local context (quantity of traffic rerouted, number of additional conflict points, and number of changes in flight levels).

The period of time during which neighbouring ATM units would reduce capacity would equally be a function of the circumstances. However, opinion is shared that it would be measured in weeks rather than in months.

The reaction of the neighbouring ATM units in terms of capacity reduction and duration of such capacity reduction is a parameter to be discussed between neighbouring ANSPs within the context of the preparation of their own contingency plans.

To the extent the reaction of neighbouring ATM units would have a material impact on the potential consequence of an outage it would be critical to establish a dialogue between adjacent ANSPs as to the magnitude of such consequences.

4.3.4 COST OF THE RESTORATION OF THE CAPACITY

To establish a reasonable order of magnitude of the cost of restoration of capacity under the "Wait and see" scenario, it has been demonstrated the impact of the cost of capacity restoration under the "Wait and see scenario" is only a fraction of the cost avoidance, hence it is of a second order of magnitude in the Economic Assessment of Service Continuity.

5. IMPACT OF OUTAGES PER STAKEHOLDERS

Economic Guidelines recommend considering each category of stakeholders separately then to consider the cumulative effect of Service Continuity mainly:

- Airspace users
- ANSPs
- Airports and local society
- Passengers

5.1 IMPACT OF OUTAGES FROM THE AIRSPACE USERS' PERSPECTIVE

Airspace users would potentially be exposed to:

- Delays on the ground
- Re-routings of flights around the Area of Responsibility (AoR) of the failing unit
- Diversions to airports outside the Area of Responsibility of the failing unit
- Flight cancellations

Airspace users having their main base of operations in the Area of Responsibility of the failing unit would be exposed to severe financial troubles

5.2 IMPACT OF OUTAGES FROM THE ANSPS' PERSPECTIVE

ANSPs where a long lasting outage would occur would be exposed to severe financial trouble. ANSPs are also exposed to public criticism, damage to corporate reputation and customer base.

ANSPs performing under the cost recovery mechanism have strong expectations that unit rates should reduce steadily: in case of a long lasting outage of one of their units the chargeable service units would decrease and the ANSP's unit rate would be severally affected all the more when airspace users would fly around the airspace, making the situation even worse.

ANSPs performing under a price cap regime linked to a performance targets have a vested economic interest in ensuring that consequences of outages are kept as low as possible.

5.3 IMPACT OF OUTAGES FROM THE AIRPORTS' PERSPECTIVE

Airports located under the Area of Responsibility of a failing unit would be severely hit by long lasting outages of the TMA.

Closure of an airport will have knock-on effects on other airports:

- Negative effects on the origin & destination airports as a direct proportion of the number of flight cancellations,
- Positive on nearby airports as a direct proportion of the number of flights diverted to such airports.

5.4 IMPACT OF OUTAGES FROM THE PASSENGERS' AND LOCAL SOCIETY'S PERSPECTIVE

Passengers usually departing or landing at airports located under the AoR of a failing unit would be potentially exposed to:

- Delays before departure;
- Obligation to use more time consuming or more expensive modes of transport, when available;
- Obligation to go to distant airports when no other mode of transport is available;
- Travel cancellations when no alternative is available.

The total impact would also include indirect societal losses (i.e linked to loss of jobs, impact on tourism and revenues from air freight) in the catchment area of the airport.

6. DESCRIPTION OF THE MITIGATING STRATEGIES FOR EACH CATEGORY OF OUTAGES

For each severe situation described above, i.e.:

- A facility is out of service but the staff is operational (flood, explosion at a moment when there is almost no staff present)
- A major software bug has occurred -
- A facility is operational but part of the staff was hit (pandemics, explosion when staff is present)

ANSPs should follow a similar process as described above for the “Wait and see” scenario:

6.1 DESCRIBE THE OPERATING CONCEPT OF THEIR MITIGATING STRATEGY (IES)

The purpose of this critical step is twofold:

- To assess if a cost effective means of protecting against the consequence of a major outage exists or not.
- In case the answer is positive to find out which strategy or combination of strategies is most cost effective or affordable.

In performing this critical exercise ANSPs should ensure that the proposed strategy (ies) is an effective response to the outages. For instance, if the ANSP wants to ensure Service Continuity in case of earthquakes, a concept of contingency based on the utilisation of a co-located operation/ contingency rooms would be ineffective.

6.2 DESCRIBE THE DURATION OF CAPACITY RECOVERY AND THE PATTERN OF CAPACITY RECOVERY

The Economic Analysis has shown than

the pattern of capacity recovery is critical. In terms of gross benefits the availability of a full back-up facility is an effective solution because it avoids most of the losses incurred until capacity is restored.

6.3 DETERMINE THE COST (INVESTMENT COST AND RUNNING COST) OF THE STRATEGY (IES)

Contrary to what happens in the "Wait and see" scenario, ***the cost of investment has a major impact on the cost effectiveness of the strategy.*** Unless the outage would occur (and to a lesser extent depending on the level of traffic), building and maintaining a full back up ACC (50 to 100 million) could be a drain of limited resources.

Economic Analysis has equally shown that the operating cost of maintaining the contingency has a significant impact on the cost effectiveness of the strategy. A system requiring continuous maintenance could prove to be very expensive. A trade-off must be looked for between the merits of a system providing at all times maximum fall-back capacity and those of a system requiring some efforts (money and time) for upgrade hence taking a longer time to produce the same capacity/service level. The Economic Analysis is capable to assist in performing the analysis of the trade-off.

Since the cost of implementing a strategy is not the only element to take into account for the decision (see below Conclusions), at least the Economic Analysis can assist ANSPs (and State authority/ policy making authority) in determining the financial envelope required for contingency planning for service continuity.

The steps describing the mitigating strategy could be summarised in a table like:

Event[9]	*Capabilities affected*	*Description of the mitigation strategy and demonstration of the fitness for purpose*	*Pattern of capacity recovery*	*Cost of proactive active actions (investment and running costs)*
Earthquake				
Flooding				
Lightning				
-				
-				
Software Bug				

Figure 36 - Description of candidate mitigating strategies for Service Continuity

7. PERFORM THE ECONOMIC ANALYSIS OF THE MITIGATING STRATEGY (IES)

The Economic Analysis has shown how critical it is to perform an economic analysis of all alternative strategies restoring part or all of the lost capacity/service level for each event of outage.

7.1 GENERAL PRINCIPLES

The performance of the economic analysis consists in comparing the costs and benefits of each "Service Continuity" strategy against the "Wait and see scenario". In an ideal world several solutions would emerge and would be ranked by orders of merits.

The analysis consists in identifying and measuring for each ATM unit, each category of outage and each candidate mitigating strategy:

- The net benefit of having "contingency in place" against the "Wait and see" scenario
- The cost (investment cost and running cost) of the mitigating strategy
- And to establish the cost effectiveness of each mitigating strategy, taking into account the probability of occurrence of the outage, the accepted discount rate, the required cost to benefit ratio and as the case may be the risk aversion factor declared by the key players and endorsed by the regulator.

7.2 PERFORMANCE OF THE ANALYSIS PER STAKEHOLDER

This exercise should be seen from the perspective of each category of stakeholders. ANSPs and regulators should open the dialogue with the stakeholders so as to collect quality inputs for the economic analysis and secure buy-in of their strategy.

The results of the economic analysis are very much dependant on some individual values used as standards for the performance of cost benefit analysis such as the CBA for SESAR.

Such figures should be fine-tuned as much as possible and made consistent. This exercise should also be undergone locally for the performance of local contingency planning and in order to secure buy-in by local stakeholders.

7.2.1 AIRSPACE USERS

The net benefit for the airspace users of any Service Continuity scenario equals the cost of disruption per day times the number of days of outage under the "Wait and see" scenario minus the total cost of disruption per day times the number of days of outage under the Service Continuity scenario:

$$benefit = (\sum_{Steps} Cost\ of\ disruption\ per\ day * Number\ of\ Days\ of\ disruption\ )_{Wait\ and\ See} - \\ (\sum_{Steps} Cost\ of\ disruption\ per\ day) * Number\ of\ Days\ of\ disruption)_{ISC}$$

Where:

- Steps indicate the intermediate phases of capacity restoration (e.g. 0%, 25%, 50%, and 75%) and
- ISC stands for "Implementation of Service Continuity".

and where:

$$Cost\ of\ Disruption\ per\ Day = Daily\ Cost(EKF) + Daily\ Cost(MsD) + Daily\ Cost(DAAs) + DailyCost(Cancellation)$$

where:

EKF = Extra Kilometres Flown; MsD = minutes of delay; DAAs = diversion to alternate airports

The net cost for the airspace users equals the cost to maintain Service Continuity in place minus the cost required to restore capacity under the Wait and see scenario.

$$Costs\ = \sum (\text{"}Contingency\ in\ place\text{"}\ costs)\ - \sum (costs\ restore\ capacity\ in\ \text{"}Wait\ and\ See\text{"})$$

The economic assessment should aim at calculating the discounted economic value of such net benefits minus net costs, at an agreed interest rate (e.g. 8%) and an agreed probability of occurrence of the outage, to compare such value to the value of the investment. The basic formula for the calculation of a discounted value at a given probability of occurrence of outage and rate of interest is of that form:

Economic value = Net Present Value of (DR;P;V/P)

Where

DR = Discount Rate; P = Probability of occurrence of outage; V= Value

From airspace users' perspective there is by definition a potential business case for a decision to invest in Service Continuity when the discounted economic value of benefits exceeds the discounted economic value of the investment.

7.2.2 ANSPS

The difference between the total loss of revenues for the ANSPs under both the "Wait and see scenario" and each candidate scenario of Service Continuity represents the benefit of having Service Continuity in place.

The impact should be assessed:

- At the network level (all ANSPs consolidated);
- At the ANSP's level: the ANSP of the failing unit will be in survival mode whilst the neighbouring ANSPs could be exposed to overload.

7.2.3 AIRPORTS

The difference between the total loss of revenues for the airports under both the "Wait and see scenario" and each candidate scenario of Service Continuity represents the benefit of having Service Continuity in place.

The impact should be assessed:

- at the network level (all airports consolidated)
- as the case may be, at the level of the airports based in the Area of Responsibility of the failing unit. These airports will be in survival mode whilst the neighbouring airports could be exposed to overload and at the same time will be in a position to book extra revenues.

7.2.4 PASSENGERS AND LOCAL SOCIETY

An impact assessment from the passengers' perspective is based on the value of time for passengers exposed to foreseen departure delays, or to the obligation to move to other airports.

An impact assessment from the society's perspective is based on the cost of CO2 emissions saved or increased further to the implementation of Service Continuity as well as on other societal costs in the catchment area of the airports based in the Area of Responsibility of the failing unit and not measured as part of the economic analysis of the airports.

[10] The scoping analysis has made use of a customised version of the EUROCONTROL EMOSIA software tool. ANSPs and their regulators should make use of an economic model of similar nature.

7.3 DIALOGUE WITH THE AIRSPACE USERS

The scoping economic analysis has shown that the cost effectiveness of Contingency Planning for Service Continuity is significantly dependant on the value of delays, cancellations, re-routings and diversions to alternate airports.

As an example, the following values of costs were considered in the simulations that supported the elaboration of these guidelines:

- Value of a minute of delay on the ground: circa €20
- Cost of cancellation: circa €8000
- Cost of diversion to nearby airport circa €4000
- Cost of extra kilometers flown: circa €5 a km;

The situation is different from one environment to the other. Each ANSP should be encouraged to open up a dialogue with the "20% of its airspace users producing 80% of the traffic" as to their expectations from contingency planning for Service Continuity and the cost items that they would recognise. Such users should offer guidance as to their preferred trade-off between delays, re-routings and cancellations and as to the cost of delays, extra kilometres, and diversions to alternate airports, cancellations, so that the economic analysis can be performed as accurately as possible.

Predictability is of importance. Airspace users can much faster fine-tune their operations if a contingency plan accurately details the progressive restoration of capacity over the coming weeks and months. Well informed airspace users may adjust the "generic" priorities described above and reduce the net cost of severe outages accordingly.

The local economic analysis should seek to simulate to a reasonable extent such preferred trade-offs and adjustment of priorities.

7.4 DIALOGUE WITH THE AIRPORTS

A similar dialogue ought to take place with the airports for which the ACC offers services.

In the end there should be significant differences in perceptions between a hub airport and a traditional airport; between an airport dedicated to low cost or charter carriers and an airport handling large spectrum of traffic.

For such reasons ANSPs and regulators should hold bilateral discussions with the airports situated in the Area of Responsibility of each ATM unit subject to an economic appraisal of service continuity. ANSPs may wish to discuss with the airports of their Area of Responsibility how they could contribute to the financing of the investment in service continuity.

7.5 DIALOGUE WITH THE STATE AUTHORITIES

Passengers and local economy

The State is the single entity in a position to take into account categories of interests that are not directly represented: passengers incapable to travel by air and forced to cancel travels or to use alternative modes of transport; regional and national economies directly or indirectly impacted by a severe outage, protection of the environment

There cannot be one single figure to account for the value of time for passengers in ECAC or to account for the passengers' cost of cancellations.The use of local inputs from e.g. local chambers of commerce should be encouraged.

Regional and national economies would be differently affected by a severe outage; high level figures are available from APAG, the Air Transport Action Group. They do not differentiate between most developed countries of Western Europe and other countries of the eastern part of Europe. Again States could use better figures when available and where this would be relevant.

Environment

The value of emissions is available to establish the net gain or loss in terms of pollutions. The economic assessment would measure the surplus of emissions due to re-routings around the failing unit and the savings due to cancellation of flights. Possibly it could consider the effect the outage may have on e.g. the utilisation of substitute modes of transport.

Others

Other values can also be taken into account such as the value of military flights and of priority flights.

8. FINALISING THE ECONOMIC ANALYSIS OF THE CANDIDATE MITIGATING STRATEGIES

Economic Analysis has shown that not all candidate mitigating strategies would be sufficiently beneficial to be retained and that some strategies are more robust than others in terms of cost effectiveness.

It could be that due to a low rate of probability of an outage no mitigating strategy will meet the criteria of cost effectiveness. ***In such cases the concept of aversion to the risk could be considered.*** Typically this aversion to risk reflects the reaction of an individual or a group to a situation where the probability of occurrence of the event is extremely low but the potential consequences of the event are very expensive. Alternatively the economic analysis would be used to determine at which discount rate or probability of occurrence of the outage the required criteria would be met.

9. SUMMARY

The logical framework for the performance of the economic assessment can be summarised as follows;

1. Hazard assessment

- List and describe the outages
- Determine the probability of occurrence of -clusters of- outages
- Perform an economic assessment of the "Wait and see" scenario

2. Develop candidate mitigating strategies for each -cluster of - outages

- Describe the operating concept of the strategy
- Describe how it matches the outages

3. Perform economic analysis of each mitigating strategy

- Dialogue with the stakeholders
- Perform analysis for each category of stakeholders
- Finalise the economic analysis: Dropping the least cost-effective mitigating strategies and rank the remainder by merits

4. Propose an informed local policy of Service Continuity

The proposed framework is visualised below.

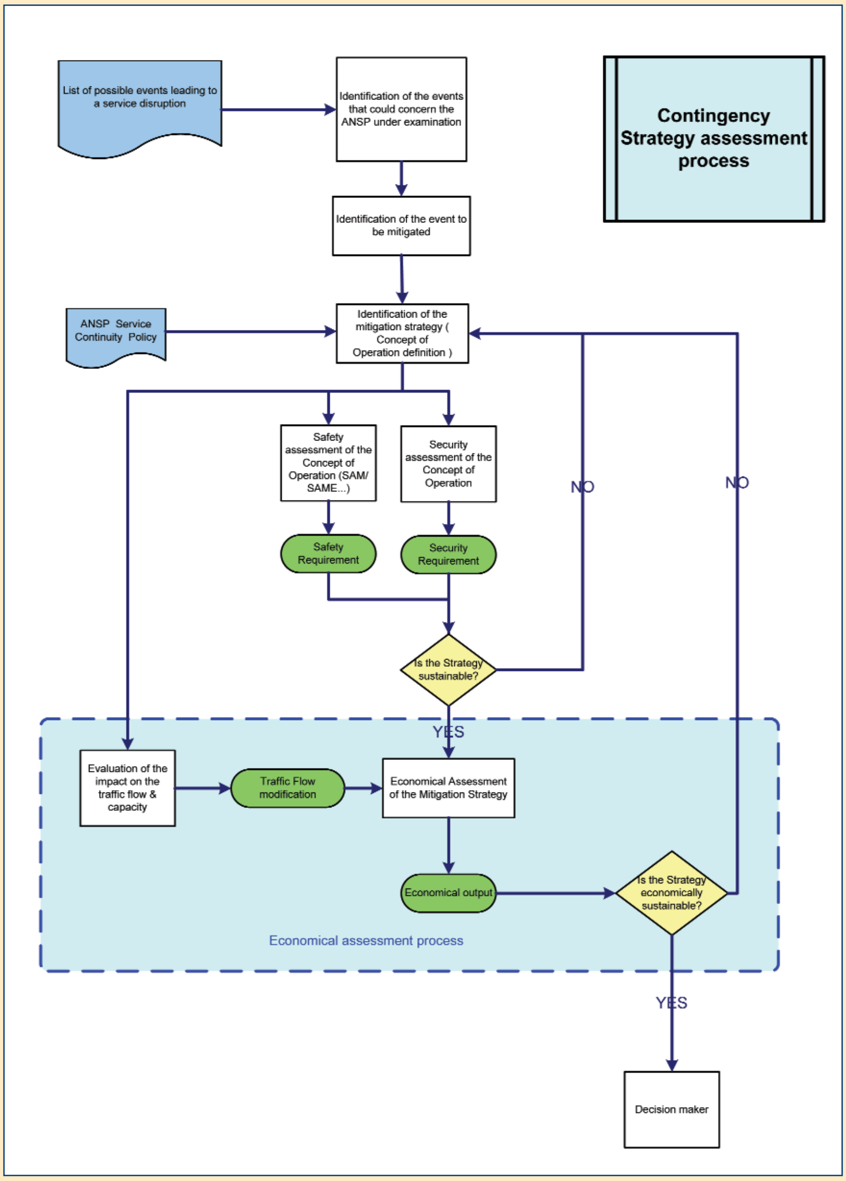

List of possible events leading to a service disruption
Identification of the events that could concern the ANSP under examination
Contingency Strategy assessment process
Identification of the event to be mitigated
ANSP Service Continuity Policy
Identification of the mitigation strategy (Concept of Operation definition)
Safety assessment of the Concept of Operation (SAM/ SAME...)
Security assessment of the Concept of Operation
NO
NO
Safety Requirement
Security Requirement
Is the Strategy sustainable?
YES
Evaluation of the impact on the traffic flow & capacity
Traffic Flow modification
Economical Assessment of the Mitigation Strategy
Economical output
Is the Strategy economically sustainable?
Economical assessment process
YES
Decision maker

Figure 37 - Overall process of assessment of Service Continuity concepts

These Guidelines should assist the ANSPs and State authority/ Policy making body in:

- Deciding to limit their policy to the provision of contingency planning for degraded modes of operations or on the contrary to expand such policy to cover the case of Contingency Planning for Service Continuity.
- Putting together the business case of candidate strategies; in these regards in identifying the key elements influencing the profitability of investment in Service Continuity.
- Establishing the financial envelope required by contingency planning for Service Continuity.

At that moment in time ANSPs and "State authority/ Policy making body" have some key elements in hand to make their final decision.

Economic Guidelines insist that the economic analysis is only a part of the decision making process in Service Continuity. No decision to invest however depends solely on the results of an economic assessment of candidate strategies.

The final decision to invest in Service Continuity should take into account but should not be limited to, other considerations such as:

- The ability to finance which may vary depending on e.g. the cost of money or the status of the industry at that time
- The need to account for limited financial and / or human resources and priority to spread the investment programmes over the years
- The possibility to link the decision to the outcome of a future technological change
- The opportunity to link the decision to a programmed upgrade of facilities
- The possibility to link the contingency planning for Service Continuity to the success of bilateral or multilateral arrangements, hence to delay the decision as to the strategy until such arrangements are in place
- The attitude of the local airspace users and airports and their willingness to endorse a risk and/or share the burden of the financing of the mitigating strategy
- Conclusions of the safety and security assessment of each mitigating strategy
- Binding nature of the legal framework
- Political decision

10. CONCLUSION

In conclusion, in order to justify the costs of contingency measures, the economic dimension can indeed be taken into account and appropriate methodologies/tools can be applied to economically assess Contingency Plans for Service Continuity.

Whilst the methodologies and tools described above set the scene and offer guidance***, it would be wrong and misleading to assume that they describe a "one solution fits all".*** On the contrary, there cannot be one single solution for each candidate ATM unit and all ATM units candidate for Contingency Plans for Service Continuity present unique characteristics. Only experience will guide to the most promising avenues.

Moreover it should never be forgotten that economic assessment is a "toolbox" in support of decision making and that no "spreadsheet management "can take into account all the non monetary components of complex decision making processes.

Finally it is endorsed that ***Safety (and Security) levels should never be traded-off at the expense of increases in Capacity and/or Flight Efficiency.***

11. SCOPING CASE: OUTAGE OF AN ACC PLUS TMA; A FULL BACK UP FACILITY

This case is for illustration only

11.1 CONTEXT

11.1.1 THE OPERATIONAL CONCEPT FOR SERVICE CONTINUITY

For illustration of the use of the method, a specific operational concept for Service Continuity has been defined:

- build and maintain a dual use 100% back-up facility, located at long distance from the principal unit;
- The facility is potentially also used as a training centre and/or R&D centre;
- The back-up facility includes both the number of working stations required to provide full capacity plus the number of working stations required for training and R&D purposes.

The ANSP is protected against the major categories of severe disruptions of external origin such that the facility would be out of service for a long period of time but the staff would be operational:

The major categories of such external events are:

- hostile attacks (terrorism),
- fire,
- extreme object collision (aircraft, meteorite),
- earthquakes
- extreme weather conditions (flooding, tornado, lightning).

This strategy does not protect against situations where a significant portion of the staff is hit: pandemics, explosion when staff is present

This strategy possibly protects, at least partially, against the occurrence of software bugs to the extent software are not updated concurrently with the upgrade of the software in the principal unit.

11.1.2 NUMBER OF DISRUPTIONS PER DAY

Simulations have allowed the evaluation of the impact of remaining disruptions (flights cancelled, minutes of re-routings and delays) under 0%, 25%, 50% and 75% capacity restoration.

Restored capacity	***0%***	***25%***	***50%***	***75%***
Flights cancelled	***1081***	***958***	***509***	***191***
Re-routings (minutes)	***2469***	***980***	***959***	***525***
Delays (minutes)	***-17061***	***-18691***	***-10247***	***-2044***

Table 38 - Scoping case - number of disruptions / day

Due to the closure of the TMA, all flights to and from the airports located in the AoR of the failing unit are cancelled then progressively restored as capacity comes back.

11.1.3 NUMBER OF DAYS OF OUTAGE

With Service Continuity in place Full back-up recovery would require a total of 30 days;

Under the Wait and see scenario, 3 years would be required to rebuild the facility

Number of days of outage				
Restored capacity	***0%***	***25%***	***50%***	***75%***
Under the Wait and see scenario	***30***	***100***	***200***	***770***
With Service Continuity		***1***	***5***	***25***

Table 39 - Scoping case -Number of days per restored capacity

11.1.4 INVESTMENT AND OPERATING COSTS

11.1.4.1 Under Service Continuity

Investment

The investment includes the cost required to fulfil the mitigating strategy: 50 million plus the cost of training and R&D functions: 5 million.

Only that part of the investment in relation to the mitigating strategy (50 million) is taken into account in the economic analysis.

Renewal of the investment - Maintenance of the investment

This investment would be renewed every 20 years. The decision to reinvest in Service Continuity ought to be confirmed each time the decision to renew the investment is taken.

The cost of maintenance of the investment is deemed to be 5% of the initial investment i.e. 2.5 million per annum.

Other operating costs

Other operating costs would include the cost of moving the staff to the full back up facility for a period of three years. This is expressed as a percentage of the total staff cost of the failing unit.

11.1.4.2 Under the "Wait and see" scenario

Under the pressure of time ANSPs would develop and implement equipment and procedures to restore some capacity at the same time as they would launch the rebuilt of the out of service facility. This cost is deemed to be 100 million.

11.1.5 PROBABILITY OF OCCURRENCE OF AN OUTAGE

The probability adopted is the average of two deterministic probabilities:

Event unlikely to occur in the life of an installation; never occurred on the site but was observed sometimes on other sites	***About 10-2 per annum***
Event shouldn't occur in the life of an installation; never occurred repeatedly on the site and was observed very seldom regularly on other sites	***About 10-3 per annum***

Table 40 - Scoping case -Deterministic probability of occurrence of an outage

On such a basis the economic analysis considers a probability of occurrence of one outage across ECAC every 500 years.In addition, Stakeholders express a degree of "aversion to the risk of chaos" and in doing so want protection against a higher probability of occurrence of an outage, e.g. one outage every 200 years.

11.2 THE AIRSPACE USERS' PERSPECTIVE

11.2.1 DAILY COST OF CAPACITY SHORTFALLS

Each day of outage would cost the airspace users the following amounts:

	Daily Costs in			
Restored capacity	***0%***	***25%***	***50%***	***75%***
Cancellations	***7 918***	***7 017***	***3 728***	***1 399***
Re-routings	***113***	***45***	***44***	***24***
Delays	***-349***	***-382***	***-210***	***-42***
Total / day (K)	***7 683***	***6 680***	***3 563***	***1 381***

Table 41 - Scoping case -Cost of disruptions / day for the airspace users

Cancellations represent the largest share of the cost at 7.9 million per day at the beginning, reducing as a direct proportion of capacity restoration.

Extra kilometres flown due to re-routings have an impact of .01 million per day, progressively reducing as capacity is restored.

Delay reductions contribute for about 5% to a reduction of the total cost.

11.2.2 ECONOMIC VALUE OF THE INVESTMENT IN SERVICE CONTINUITY

Net benefit

The benefits for the airspace users of having a dual 100% back up facility available within a month equal 2.7 billion.

Assuming a probability of occurrence of one outage every 200 years and a discount rate of 8% the discounted cash flow of such benefits of 2.7 billion is about 170 million.

The present value of the renewed investment -renewal every 20 years - plus maintenance of such equipment is about 45 million.

The net benefit of Service Continuity is therefore 170 million minus 45 million: 125 million.

In such a situation, an investment of 50 million in such full back up facility presents a CBA ratio of 2.5:: 1 at the level of the airspace users.

11.2.3 RISKS AND SENSITIVITY

The value of the investment is highly sensitive to key inputs such as:

- The value of cancellations, due to the very large number of cancellations;
- The probability of an outage;
- The total number of days of disruptions;
- The renewed investment and the cost of maintenance of such investment.

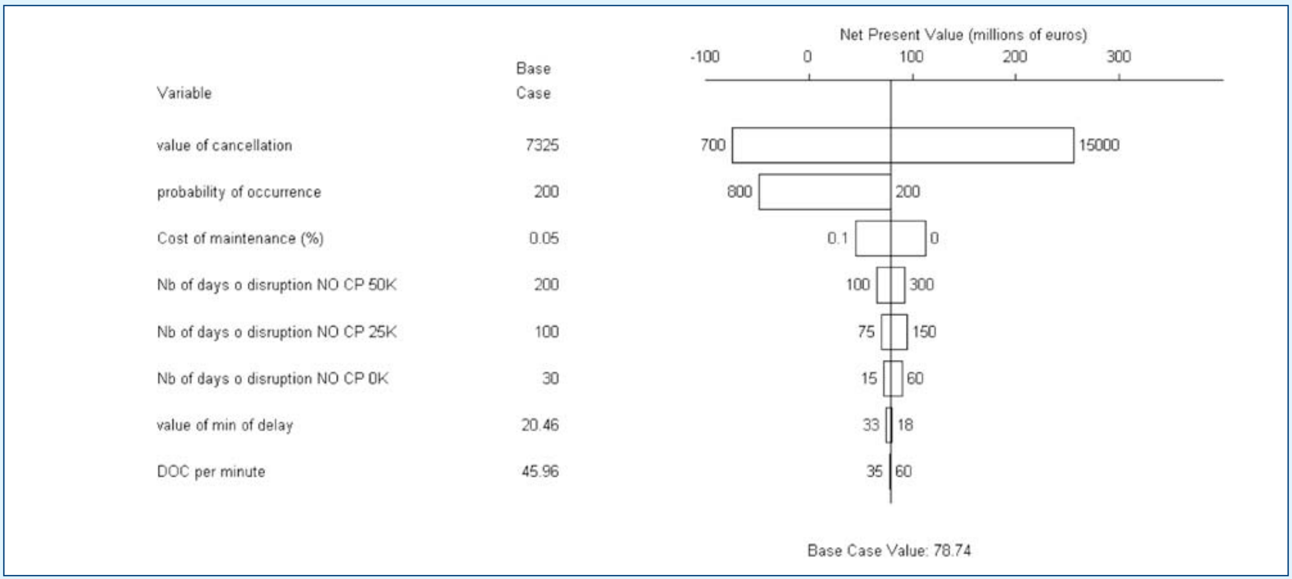


Table 42 Scoping case -Sensitivity analysis

11.3 THE ANSPS PERSPECTIVE

11.3.1 AT THE NETWORK LEVEL

Each day of outage would cost the ANSPs the following amounts:

The net benefit for the airspace users of having a dual 100% back up facility available within a month equal 280 million.

Assuming a probability of occurrence of one outage every 200 years and a discount rate of 8% the discounted flow of such lost revenues of 280 million is about 17 million.

Restored capacity	***0%***	***25%***	***50%***	***75%***
Loss of revenue / day for the ANSPs (K)				
Cancellations: en-route	***617***	***547***	***290***	***109***
Cancellations: TMA	***223***	***197***	***105***	***39***
Re-routings (minutes)	***-16***	***-6***	***-6***	***-3***
Total / day (K)	***823***	***738***	***389***	***145***
Days spent in « Wait and See » Scenario	***30***	***100***	***200***	***770***
Days spent in "Contingency in place » Scenario		***1***	***5***	***25***
Benefits in K	***24690***	***73062***	***75855***	***108025***

Table 43 - Scoping case -Cost of disruptions for ANSPs at network level

11.3.2 AT THE LOCAL LEVEL

The ANSP of the failing ACC-TMA would lose 50% of the TMA revenue. Moreover, on the assumption that ECAC wise a flight crosses in average the airspace of three ANSPs, such ANSP would lose one third of the En-route revenue. In total it would lose 110 million.

11.4 THE LOCAL AIRPORTS PERSPECTIVE

Assuming reference annual revenue of the main airport directly hurt by the closure of the TMA of 370 million, the combined loss of revenues of all directly concerned airports could be as follows:

Assuming a probability of occurrence of outages of one every 200 years and a discount rate of 8% the discounted cash flow of such benefits of 681 million is about 43 million.

Subject to the assumptions, the CBA ratio of an investment of 50 million in a 100% back up facility, whilst presenting a CBA ratio of 2.5::1 at the level of the airspace users, would be increased by 0.8::1 as a maximum when the airport level would also taken into account.

Restored capacity	***0%***	***25%***	***50%***	***75%***	***Total***
	Direct Loss of revenues (K)				
Without Service Continuity (K)	***45 616***	***114 041***	***152 055***	***292 705***	***604 418***
With 100% back-up facility	***0***	***1140***	***3801***	***9503***	***14 445***
Gross benefit					***589 973***
	Indirect & induced effects 15 %				
Loss of revenues	***6 842***	***17 106***	***22 808***	***43 906***	***90 663***
Net benefit	***52 459***	***130 007***	***171 062***	***327 108***	***680 635***

Table 44 - Scoping case -Cost of disruptions for local airport

- Without Service Continuity in place, airports lose 604 million direct revenues plus 90 million indirect and induced revenues as a consequence of the flight cancellations.
- With Service Continuity in place direct losses would be limited to 14 million.

- The net benefit of Service Continuity is 681 million.
- There should be only losers: airports in the AoR of the ACC-TWR would be exposed to financial chaos; origin and destination airports would as a minimum lose regulated charges and ancillary revenues as a consequence of the cancellations.

11.5 THE PASSENGERS PERSPECTIVE

As indicated in sections 7.2.4 Passengers and local society and 7.5 Dialogue with the State Authorities above this would be determined locally

11.6 THE GLOBAL PERSPECTIVE

The economic analysis gives some elements to support decision-making:

- An investment of 50 million in such full back up facility presents a CBA ratio of 2.5:1 at the level of the airspace users.
- The ANSP would save 280 million.
- Significant airport benefits - 680 million- accrue to the airports located in the AoR of the failing unit.

APPENDIX I - SPECIAL CASES

1. GENERAL

It is important to stress that the strategies described in Appendix C - ANS Contingency 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 centralised facilities that require staff to move from an affected centre would not provide ideal solutions to pandemic contingencies. Various types of 'common mode' failure can introduce additional vulnerabilities and concerns that require special planning arrangements to be made. Moreover, it is generally acknowledged that the industrial action creates a different dynamic within which national administrations and ATS providers must work.

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 minimise 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.

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 area . 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

[11] 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.

SPECIFIC REQUIREMENTS

PLANNING

PREPARATION OF PLANS

- 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

- 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)

- 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

- 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

- 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 premised on regular basis.

RECOVERY

Phase 5: Longer-Term Response and Recovery

- 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

- Revise contingency plans to consider subsequent outbreaks as soon as possible.

Figure 45: Case Study of Planning for Pandemics (Strategy Neutral).

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).

The previous shows how the Framework for execution of contingency plan (see 11.2 Execution of the Contingency Plan) 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 x but is included as an alternate perspective and to retain consistency with the other strategies detailed in Appendix C - ANS Contingency Strategies. It is important also to note that Figure X 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. 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 Appendix C - ANS Contingency Strategies. 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.

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.

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 this document

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

7. INDUSTRIAL ACTION

From a User point of view disruption of the provision of ATS resulting from industrial action or strike does not differ much from the one caused by technical/catastrophic outages, except, of course, that the former case normally follows a period of prior notification.

It is generally acknowledged that the lack of ATS as a result of industrial action creates a different framework within which national administrations and ATS providers must plan. It must be recognised that industrial action creates a need for advance plans quite different from those in respect of technical/catastrophic failure.

Arrangements for contingency planning in respect of industrial action need to be treated independently of other plans, and must remain within the limits permitted by national legislation and constraints as explained in this chapter.

The right to strike is recognised as a basic acquisition in many States and is therefore included in their respective Constitutions. From a more international perspective the right to strike is addressed in the documentation of various legal instruments, e.g.:

- the "International Covenant on Economics, Social and Cultural Rights" adopted by the United Nations in 1966;
- the "European Social Charter" adopted by the Council of Europe in 1961 and revised in 1996;
- the "Community Charter of the Fundamental Social Rights of Workers" and the "Charter of Fundamental Rights of the European Union" adopted under the auspices of the European Community in 1989 and 2000 respectively.

International and national legislation, proper to a State and normally of a complex nature, are then translated in varying resolutions or decrees notifying the determination of each individual State. It should be remembered that each State must address industrial outage within the context of its unique legal conditions. As a result, it is not, within the context of this document, possible to standardise how States might plan for or react to industrial action.

Having accepted the unique nature of each State's legal situation, in strategic planning for industrial action, it should also be remembered that the objective should be to maximise the capacity of the ATS system as a whole, and not necessarily only address the numbers of flights which can be accommodated in the affected airspace.

Again, what follows should therefore be interpreted as a catalogue of Guidelines for consideration by States, rather than an enumeration of requirements.

- Noting the safety hazards of sudden interruption of the provision of ATS in a State, but also in adjacent States (sectors) it is advisable to notify the aviation community of (potential) industrial action in due course. A pre-warning of 24 hours is considered as the minimum. Some States require much larger periods, varying from 5 up to 10 days. When determining the pre-warning period, consideration should be given to (excessive) long periods, which may cause premature changes on the traffic flow planning, should the industrial action be cancelled.
- Respect of international engagements; in some States priority is given to overlying traffic (not landing in or taking off from the State subject to industrial action). States should look at this item whilst negotiating with the unions.
- It should be realised that the consequences of disruption of ATS in a sector or a unit can not be isolated to that sector, but could be detrimental for the whole ECAC air traffic flow (management).
- 'Where service providers consider it appropriate, and in accordance with national legislation, they could negotiate agreements with staff on minimum service levels which would help the CFMU in its contingency role. However, other States should have the option to retain the freedom to deal with the consequences of industrial action on a tactical basis. States and/or service providers may find it appropriate to consider whether or not minimum levels of service should be included in their planning. Moreover, a State or service provider should have the flexibility in deciding when and in what conditions the minimum level of service agreement is implemented.

An example of a possible list of essential elements to be considered in planning for contingencies in the event of industrial action is given below. Adherence to all or some items of the list hereafter is considered being a prerogative of States:

- Aircraft in a state of emergency;
- Search and rescue and humanitarian/medical flights;
- Safeguard national interest and goods. Preserve the rights of those services considered essential;
- Ensure safety of persons and goods, maintenance of premises, machinery, installations...
- Continuity of support to the Military ATS and or Air Defence structures (flight planning...);
- Minimise to the extent possible, the effects of industrial action on traffic overlying

8. VOLCANIC ASH

A strong misconception amongst ANSPs is that volcanic ash does not affect them when there are no volcanoes in or near to their territory. However volcanic ash travels for thousands of miles and the ash cloud itself can be in excess of 2000 miles long. Examples of volcanic ash affecting aircraft include a B747 over Chicago Illinois damaged by ash from the Philippines and a DC9 on descent into El Paso, Texas damaged by volcanic ash from Alaska.

Within Europe, volcanic activities in Iceland, Italy, Canary Islands and the Azores all pose a potential threat. In response ICAO has produced a Volcanic Ash Contingency Plan which it considers to be an ATS contingency plan. The Reference for the document is ICAO EUR Doc 019 which can be downloaded from:

http://www.paris.icao.int/Volc_Ash/docs/EUR%20VA%20CP_rev20080904.pdf

In addition, further information and advice for ANS providers can be found:

- on the ICAO EUR & NAT web site http://www.paris.icao.int/Volc_Ash
- in ICAO Doc 9766, International Airways Volcano Watch, and
- in a paper presented by IATA at the ICAO ATM/AIS/SAR/SG/15 meeting held in July 2005, Contingency Planning for Volcanic Eruptions.

The safety implications for aircraft routing through volcanic ash clouds are well known and obvious. ANSPs are encouraged therefore to consider the information providing in the Reference material in particular with regard to their coordination with the Volcanic Ash Advisory Centres/Meteorological Watch Offices, AOs and CFMU.

Moreover, ANSPs should take active part in the volcanic ash exercises organised in their areas of responsibility, to ensure their readiness in case of an actual volcanic ash activity.

APPENDIX J - CONTINGENCY PLANNING FREQUENTLY ASKED QUESTION (FAQS)

This Appendix aims to provide answers, backed up by references within these Guidelines, to numerous Frequently Asked Questions (FAQs) concerning ATM Contingency Planning. References from within this document and other external sources are provided. Three areas are covered:

- Legal and Regulatory
- ATM Security
- Training and Testing/Exercising

1. LEGAL AND REGULATORY

1. Which type of services provided by ANSPs should be covered by contingency plans?

Annex 11 to the Chicago Convention requires contingency plans for air traffic services (which include flight information service, alerting service, air traffic advisory service and air traffic control service).

Regulation (EC) No 2096/2005 requires contingency plans for all the services provided by the air navigation service provider. In accordance with the SES definitions, air navigation service providers are entities providing air navigation services (ATS, MET, AIS, and CNS) for general air traffic. The question of application of contingency plans to other services provided by ANSPs but falling outside this definition (e.g. ASM, ATFM) remains open.

Article 4 of (EC) Regulation N° 2096/2005 foresees the possibility of limited certificates for ANSPs not providing cross-border services. The limited certificate allows certain derogations, for instance relating to the requirements for contingency plans. As a consequence, and subject to compliance with derogation conditions, not all air navigation service providers are obliged to have in place contingency plans.

2. The Common requirements Annex I § 8.2 provide that ANSPs shall have in place contingency plans one year after certification, but they don't give any information on how the NSAs shall approve these plans: How should the NSA approve the plans?

The NSA needs to check the existence of the plan and its appropriateness to the ANSP level of service provision. It also verifies that the plan is effectively put in place / prepared by the ANSP.

For this purpose, the NSA will have to define in advance and communicate to the ANSP the criteria/requirements against which it will assess the Contingency Plan. This allows the ANSP to know what may constitute or not an acceptable means of compliance to meet the requirements. EUROCONTROL Guidelines (as well as local guidelines, e.g., MUAC 4 States AMC and Analysis of Common Requirements) can be used by the NSA to define their own specific requirements, but do not constitute per se binding acceptable means of compliance.

3. Will the NSA verify only the existence of the plan, or will it verify its substance and decide whether it is adequate?

The NSA will check existence and verify the substance of the plan (that all the services are covered, the identified cases of disruption, mitigation measures for identified cases, practical test) and evaluate if the plan is adequate.

They will check if the ANSP works following the plan, the internal procedure (e.g. the list of causes for disruption in Appendix B- List of Events to Support Risk Assessment and the stepped approach in Chapter 8 - Contingency Planning Process in the EUROCONTROL guidelines could be used).

4. Should the approval be given separately? Should it be formalised in a specific document?

No separate document is needed.
The approval is a part of the whole certification process. It can be treated in a specific chapter in the audit report and with a statement if it is adequate or not. This approval fits into the framework of the supervision and the ongoing oversight.

5. How does this approval fit within the on-going oversight process?

The ANSP is able to demonstrate to the NSA that all parts of the plan have been implemented and that they are effective (feasibility tested and validated, preparedness for contingency situations maintained, training program available for all relevant aspects of the contingency plans, security aspects addressed).

6. What happens if the plan is not sufficient / not approved?

In an ongoing oversight phase, the NSA can decide to organise intermediate auditing more frequently. The ANSP must develop and implement a corrective action plan. If no remedial action is taken, sanctions could be taken according to national law.

7. How to perform oversight of contingency plans for multiple ACC?

The following scenarios are possible:

- Multiple ACC in one country: the NSA can audit the ANSPs and check contingency planning during ongoing oversight by sampling several ACC out of the total group in order to get an idea of the overall performance.
- Multiple ACC in cross-border provision of services during contingency: coordinated ongoing oversight (to check that the provision expected by the considered failing unit is effectively delivered by the relevant aiding unit). This is part of the agreement with neighbouring NSAs as mentioned in article 2.4 of the Service Provision Regulation.
- Multiple ACC in several countries (inside one FAB): the NSAs of the States involved audit the ANSPs and check contingency planning during ongoing oversight by sampling several ACC out of the total group in order to get an idea of the overall performance. This is part of the agreement between NSAs as mentioned in Article 2.4 of the “Service Provision Regulation” and should be in line with corresponding provisions in the States' FAB Agreement (see EUROCONTROL FAB Model Agreement for an example).

8. Who gives the list of addresses to be notified when there is an outage and an ANSP will discontinue providing the service?

The ANSP is responsible to develop a list of addresses and to ensure that the list is part of the contingency plan.

9. Which minimal set of info should be delivered to neighbouring state in the event of contingency plan activation?

In coordination with the regulator, the ANSP should fix the minimal set. The nature and scope of the set of information to be exchanged must be discussed with the neighbouring State and the results have to be documented in a formal arrangement.

The minimal set of info will depend on the specific incident and the capability of each ANSP to respond to its own problem. The exact set of information and time of delivery should be agreed at ANSP level. NSAs should confirm that the agreed actions are sufficient for the contingency plan(s).

These elements are addressed in broad terms in the EUROCONTROL Model State Agreement for FABs and delegation of ATS but in practice, it could be addressed as necessary in the Agreements between ANSPs (for instance LoAs, or Contingency Arrangements - see Model Agreement attached in Annex F to the Guidelines).

10. Is there a duty of care on a neighbouring state to a failing state if no other LoA or agreement exists?

The duty of care principle, which derives from English tort (law of negligence), posits the existence of an obligation not to cause damage to third parties, either by one's own negligence or fault.

In the absence of any prior agreement between the States, they do not owe each other a duty of care:

- *States' responsibility is limited to their own territory and airspace. The only possible duty of care would be related to diverted aircraft.*
- *Any action in execution of a duty of care could be in conflict with the sovereignty principle.*
- *Help can only be provided to the State following agreements previously established.*

In the absence of prior written agreement at State level, a given State has no responsibility based on its own provider providing services in foreign airspace or a foreign FIR.

11. What about liability issues in cross border operations?

Provisions on liability are an obligation in the arrangements between ANSPs involving delegations of services, under Regulation (EC) No 2096/2005, Annex I, § 7.

The cross-border context of such arrangements, for instance for contingency, reinforces the need for written liability provisions.

Delegations of services do not in principle lift/remove the responsibilities and potential liabilities of the delegating ANSP (failing ANSP), which remains the one originally designated by the State in which airspace the ATS is provided. Should the delegating ANSP be held liable, it would have a right of recourse against the delegated ANSP. The above-mentioned written arrangements should organise the liability between the ANSPs. They can however not arrange the right of actions of the potential victims (e.g. competent courts, applicable laws, liability regimes open to these victims).

Please refer to 5.5.1 Liabilities of the EUROCONTROL Guidelines for an exhaustive analysis of this question.

12. Who has legal responsibility in cross border incident investigation?

The incident and accident investigation shall be conducted in accordance with Annex 13 to the Chicago Convention, as well as with Council Directive 94/56/EC of 21.11.1994, where applicable.

In principle, the State where the occurrence happened is responsible for the investigation. Other States may also participate to the investigation.

It is recommended that States/ANSPs cover this aspect in the Contingency agreements (or in the agreements on delegations of ATS).

13. What is the legal position of an ATCO involved in an accident when working under degraded Modes or Contingency?

In the case of an accident, ATCOs can be subject to civil and/or criminal liability.
The civil liability aims at compensating damages suffered by victims. Very often, the employer (ANSP) would cover for this compensation, on behalf of its staff member.

On the contrary, the criminal sanctions against an ATCO cannot be covered by another person (physical or corporate).

The legal position of each ATCO is dependent on the national legal framework in which he/she is operating and needs to be investigated individually. As a general rule, the adherence to the operational rules, manual procedures and administrative instructions issued to them, as well as with the reasonable standards of behaviour (demonstrating "due diligence") is a means to mitigate the liability risks, both in normal and crisis situations. In degraded or contingency mode of operation, ATCOs involved in an accident would remain liable, but the verification of the level of due diligence exercised by the ATCO would probably take more importance and be assessed against the particular and difficult context.

14. Will the common ATC licence permit cross national border operation? Could ATCOs licence be "adjusted", e.g. in case of ATS delegation? Who takes precedence (State) when neighbours have different licensing rules for ATCOs?

Directive 2006/23/EC on a Community air traffic controller licence establishes the principle of the mutual recognition of ATCOs licences in order to ensure the free movement of these workers in the EC. However, in a contingency context, and particularly in a cross border environment, the mutual recognition needs to be completed ("adjusted") by specific competence scheme, both with regard to the minimum skills requirements (e.g. language) and to the ratings and endorsements. In addition specific training on contingency aspects needs to be provided to the ATCOs.

Detailed information on these issues is provided in the EUROCONTROL Guidelines under 10.2 Human Resources related aspects.

15. Can the ANSP which has been delegated some services, sub- delegate these services to a third ANSP?

Here again the content of the arrangements is left to the discretion of the Parties.

In principle, an ANSP may sub-contract the provision of services to a third service provider provided that:

- *this subcontractor is certified;*
- *the delegating ANSP (and also the States concerned) formally approve the sub-contract*
- *this arrangement is supported by written agreements, properly reflecting in particular the allocation of liabilities;*

This is consistent with Article 10 of the Service Provision Regulation, as well as with §7 of Annex I to Regulation (EC) No 2096/2005.

16. For cross-border activities, which regulator will regulate, or which rules will be applied?

In the absence of prescriptions in this regard in the international or European legislation, this issue should be left to the discretion of the Parties and covered in the relevant agreements (State-level agreements or agreements between service providers endorsed by the States).

These should define the applicable rules and procedures to clarify the regulatory context. Applicable rules would most likely be those of the State in which the services are provided, however, nothing prevents the Parties to decide otherwise (provided that the concerned State(s) agrees).

With regard to oversight and supervision, each NSA remains responsible for the continued supervision of the ANSP it certified. As addressed in the guidelines, § 6.3.3, NSAs have to conclude appropriate arrangements for close cooperation with each other to ensure a coordinated oversight of cross-border provision of services and contingency aspects.

17. Which regulator prevails in a cross border standards dispute or difference?

Dispute resolution between States is a difficult matter which depends on a number of factors (such as respective oversight exercised, place of the incident/accident at the origin of the dispute, content of national laws, etc.) and which can be defined in the relevant agreements beforehand.

18. Is there a public service obligation on ANSPs to provide ANS according to a set of fixed (e.g. capacity, efficiency) criteria?

If so, is there an obligation on ANSPs that intend to discontinue the services because of an outage (fundamental loss of power, control over their essential facilities) to notify the competent authorities before ANS are discontinued?

Pursuant to Regulation (EC) No 550/2004, namely article 8 thereof, the rights and obligations (such as the performance of the service in terms of capacity, efficiency, etc.) should in principle be defined by the State regulator and attached to the designation. The designation (under the form of a law, a regulation, a contract, etc.) could at the same time define the "force majeure" situations preventing the ANSP to deliver the services, as well as the possible obligations/exemptions regarding notification of the outage. ANSPs are invited to verify the existence of such provisions in their designation.

19. How do we involve ICAO when FIR boundary is over High Sea? How to involve ICAO? Is there an obligation to notify to ICAO any contingency plan implying the use of High Seas?

The involvement of ICAO in contingency planning is described in Annex 11, Attachment C, Section 5. In particular, paragraph 5.2 is relevant:

“Accordingly, States which anticipate or experience disruption of air traffic services and/or related supporting services should advise, as early as practicable, the ICAO Regional Office accredited to them, and other States whose services might be affected. Such advice should include information on associated contingency measures or a request for assistance in formulating contingency plans.”

In accordance with the same Attachment (§ 2), while contingency plans do not necessarily constitute amendments to the regional air navigation plan to be approved by the ICAO Council, they are considered as temporary deviations to the approved regional air navigation plans, because they generally involve a reduced or modified level of services.

As a consequence, in the case of the high seas airspace, any contingency plan intended to provide alternative facilities and services, involving a temporary deviation from the approved air navigation plan, must be approved by the President of the ICAO Council on behalf of Council.

20. Could Temporary restricted airspaces be started by any involved country?

In the case of the territory and territorial waters of a State, the State concerned can establish a restricted area, temporary or otherwise.

If some agreements exist with neighbouring States or ANSPs for contingency in the airspace above the territory or the territorial waters, “any involved country” (or ANSP) would need to comply with such agreement. However, in the case of high seas airspace no State can establish temporary restricted airspace. In Annex 2 - Rules of the Air, the definitions of “restricted area” and “prohibited area” clearly indicates that they can be established “above the land areas and territorial waters of a State”, i.e. not over the high seas. In the case of “danger area” there is no such restriction.

21. What is the difference between delegation of services in the High Seas airspace during normal operations and during contingency operations?

Annex 11 provides for the delegation of authority from one provider State to another provider State with regard to air traffic services in its sovereign airspace. However, as regards the high seas, it is the ICAO Council which in accordance with Annex 11 allocates specifically the responsibility for the provision of air navigation services to a provider State. This is done in the form of a "regional air navigation agreement" approved by the ICAO Council.

Consequently, a State can not delegate this allocated responsibility in the airspace over high seas to any other State.

However, a State which has accepted the responsibility to provide air traffic services in airspace of the high seas or areas of undetermined sovereignty can designate the authority (another State or an ANSP) responsible for providing the services (Annex 11, 2.1.3), on the understanding that the State retains the final and overall responsibility for the services.
Subject to the approval of the State, the designated "authority" (ANSP) could sub-designate the (normal) provision of ATS to another ANSP. Since the responsibility for the provision of ATS in this airspace remains with the State originally allocated by ICAO, and provided that the level of services remains the same, such sub-designation would not constitute an amendment nor a temporary deviation from the approved regional plans, and there would be no need to notify ICAO.

The responsibility for contingency action in the airspace over the high seas rests with the State normally responsible for this airspace (ICAO Annex 11, Attachment C, § 3.2). Contingency plans involving the ANSP designated by this State and, where applicable, other ANSPs (as aiding or failing ANSPs) remain under the responsibility of that State, but in most cases involves a variation of the level of services. Such changes are considered as a temporary deviation to the approved regional plans, and require the approval of the President of the ICAO Council.

Where possible, the approval of the contingency plan in the airspace over high seas should be sought when the outage is imminent.

In addition, ICAO Assembly Resolution A36-13, Appendix M - Delimitation of Air Traffic Services (ATS) Airspaces, Associated Practice 2 states: ***"The Council should encourage States providing air traffic services over the high seas to enter, as far as is practicable, into agreements with appropriate States providing air traffic services in adjacent airspaces, so that, in the event the required air traffic services over the high seas cannot be provided, contingency plans, which may require temporary modifications of ATS airspace limits, will be available to be put into effect with the approval of the ICAO Council until the original services are restored."***

2. ATM SECURITY

1. What is the relationship between 'Contingency' and 'Security'?

Both, Contingency and Security next to Safety can be subsumed under the wider umbrella of corporate (business/organisational) risk management. Moreover, at a very fundamental level security can be viewed as both a cause or trigger of vents that might lead to contingency situations and as an integral part of the measures and controls detailed in a Contingency plan.

The risk based approach has developed in the ATM Sector over the recent years and aims at the establishment of a sound system for internal control, remedy and review of risks to the organisation and its service delivery. Hence 'contingency' and 'security' revolve around the concept of Service Continuity and the management of resources to prevent, prepare, respond and recover from incidents impacting the achievement of this objective.

The identification of risk is important not only to ensure that resources are allocated to the best effect, but also to ensure that responsibility for management action is held at the right and most appropriate level.

Dependent on the organisation of an ANSP, contingency and security might be managed under the umbrella of separate management systems or these management systems are aligned to each other.

The risk based approach requires a continuous review of optimising performance and improvement. This encompasses the review of the processes, addressed risks and associated activities and practice.

It is therefore paramount to

- *Assess sources and classes of risks and the management of these risks in the indentified business process (e.g. safety, contingency, security, etc.);*
- *Identify links and interdependencies ensuring that the chosen measures are consistent and do not interfere/negatively impact other measures('system-wide consistency); and*
- *Ensure a stringent lessons learnt as part of the post-event analysis.*

[References: Contingency Planning Guidelines, ATM Security Management System Handbook (including associated guidance material]

2. What are the key ATM Security aspects that will impact Contingency Planning considerations?

ATM Security covers 2 major areas: Self

Protection and Collaborative Support.

Self Protection guards the ATM System against threats aimed at the ATM system and its facilities(including network, personnel and information/data). Collaborative security support is to the coordinated actions of relevant civil and military authorities responsible for countering aviation security incidents, crises and emergency situations.
[Reference Contingency Planning Guidelines chapters 7.4.1.3 Security: and 10.3 Security (Collaborative Support and Self-Protection).]

3. What level of Security should be applied during Contingency Operations?

The reference level of security is the level of security when working under "Normal' operating conditions

The requirements for ANSPs to be able to fulfil their Self Protection and Collaborative functions do not disappear during Contingency Operations. For instance in Air Policing type scenarios where a Security event is the trigger of ATM Contingency then flight plan information must still reach air defence centres for identification purposes, otherwise those flights will be classified Unknown and could be intercepted. [References: Contingency Planning Guidelines 7.4.1.3 Security:]

Moreover, Levels of security are achieved through a mix of measures/controls (security in depth, layered security). On this basis an equivalent level of security can be achieved by applying a different mix/set of measures. Accordingly, the same level of security does not necessarily imply the same controls. For instance in the case of relocation, it may be that the physical measures (e.g. perimeter fencing, barriers, control of access etc) at the alternate location are not as robust as for the primary facility. Mitigation measures might therefore include additional security patrols (by local police and/or private security firms) and alternative access arrangements such that the overall level of security is considered to be the same as during 'normal' operations).

4. Is the Security Management System framework described in the EUROCONTROL Sec MS Handbook compatible with the Contingency Planning framework in the EUROCONTROL Contingency planning Guidelines?

Yes. They are both based around a "Plan-Do-Check-Act" type cycle common to systems where continuous improvement/adaptability is necessary to manage and maintain performance.

Fundamentally, both frameworks have been devised from the classical framework used for Safety Management systems.

5. Contingency and Airspace Security

Airspace Security is a national responsibility and is concerned with the safeguarding of the airspace from unauthorised use, intrusion, illegal activities or any other violation.

Dependent on the national arrangements, ANSPs are involved in airspace security in a supporting role. The associated activities can be considered as services provided to the respective national authority. Thus, in the event of a contingency measures have to be established to ensure the provision of these support functions (e.g. air policing: flight plan information must reach air defence centres for identification purposes). [Reference Sec MS Handbook and Contingency Planning Guidelines Chapter 7.4.1.3 Security:].

ANSPs shall agree with the respective national authorities on the provision of these support services, explicitly with a view to service levels in the event of a contingency situation. National security considerations may gain primacy over the normal handling of civil air transportation. In these circumstances it might be required to change certain SOPs, rules and conventions. ANSPs should agree with the respective national authorities on the associated rules of application. Matters are addressed under the umbrella of 'Security Incident Management' (SIM) and further guidance can be obtained through NEASCOG (NATO/EUROCONTROL ATM Security Coordinating Group) or from the respective national authority. [References: Contingency Planning Guidelines Error! Reference source not found.].

6. Network and Information Security

There is a rich body of knowledge on information and network security (e.g. NIST, ISO, EUROCAE WG72, EUROCONTROL ICT Security Guidelines).

EC regulation 2096 requires ANSPs to establish an appropriate Security Management System including the protection of operational data/information.

Guidance on network and information security aspects of CNS equipment/systems can be sought through the ATM Security Team channel. As part of the on-going security risk assessments and in close cooperation with NATO/military authorities additional guidance will be developed.

Further general information regarding network and information security can be found at the ENISA (European Network and Information Security Agency) website: http://www.enisa.europa.eu).

7. How do we integrate the Security Assessment Methodology (Sec AM) into Contingency Planning?

The Sec AM can be used to deal with the specific Security threats identified in the Planning process described in the Contingency Planning Guidelines Chapter 8.

Specifically, the Sec AM can be used to support the Planning Steps 1-5 in Chapter 8 and in some parts there is a direct mapping of processes.

8. How can we get Security and Contingency to 'talk the same language'?

Harmonising the definitions and terminology used across the two disciplines would be an advantage. The Security related terms used within these Guidelines are defined in Appendix L Safety and Security Terminology Related to ATM Contingency Planning.

9. How do we balance the "Need to Know" principle enshrined in Security literature and the need to create appropriate awareness of contingency plans amongst ANSP personnel?

This can be tricky and is a matter for local management.

Plans should be made widely available to ensure that people are adequately aware of and prepared for contingency operations but disclosure should not jeopardise any business/commercial interests and sensitivities.

10. The protection of National Critical Infrastructures (which may include ANS assets) transcends Security and Contingency Planning, how should ANSPs reconcile this activity?

Various States have embarked on a national critical infrastructure programme reviewing and updating the identification and classification of 'national' critical infrastructure and associated protection programmes. These programmes typically include critical information infrastructure. ANSPs should enquiry information from the appropriate national authority.

In addition to national programmes, the EC started investigating the corner stones for a European Programme for Critical Infrastructure Protection (EPCIP) in late 2005. This issue is treated at the moment by the EC within strict confidentiality rules regarding the identification of 'European' Critical Infrastructure. European ANSPs are recommended to contact their appropriate national authority for information on EPCIP.

Further general information regarding network and information security may be found at the ENISA (European Network and Information Security Agency) website: http://www.enisa.europa.eu).

3. TRAINING AND TESTING/EXERCISING

3.1 TRAINING

1. What guidance is there for training for contingency?

There is no specific existing guidance for contingency per se.

However, the following references provide an indication of the key areas that should be covered by ATCOs as part of their training to handle emergency/degraded/unusual situations:

- *EUROCONTROL Guidelines for ATCO Common Core Content - Initial Training which lists the key operational areas to be addressed concerning the handling of Unusual/Degraded/Emergency situations.*
- *EUROCONTROL Guidelines for Controller Training in the Handling of Unusual Incidents can be found at: http://www.eurocontrol.int/humanfactors/public/site_preferences/display_library_list_public.html#newt11.*
- *EUROCONTROL e-learning package can also be accessed at http://elearning.eurocontrol.int/cnr/browse.do?c=5222 .*
- *ESARR 5 (Para 5.2.2.6.c) states that these skills should be reinforced as necessary through "periodical refresher and emergency training".*

See also Contingency Planning Guidelines, 10.2.2 Training for Contingency Modes of Operations.

2. Is there a difference between training for Emergency/Immediate Actions & Service Continuity modes of Contingency Operation

Yes. The "Contingency Life cycle" differentiates between the needs to train for Emergency Modes/ Immediate Actions and Service Continuity. Essentially as described in Q1 above, the training for the Immediate Actions as far as ATCOs are concerned would for the most part most likely be covered by their day-to-day training in that they should be able to deal with unusual situations, emergencies and de-graded modes of operation as described for instance in the EUROCONTROL Common Core Content Guidelines. Similar principles could be applied for Technical staff. However, for Service Continuity, much will depend on the strategy and measures taken to sustain operations and the level and depth of training will vary and can only be agreed at a local (ANSP) level.

3. Should there be standards for training for Contingency?

As stated above, there is guidance to cover training for emergency/degraded/unusual situations. For Service Continuity, any training will be very much dependent on the contingency measures to be put in place and any training to ensure that personnel are ready and capable of doing so can only be decided at the local level. However, in the context of a FAB agreement the partners may decide that common standards may be desirable but it is for the participants to decide.

4. How do we ensure ATCOs know about and support contingency plans?

Through training and by increasing awareness of Contingency across organisations.

See also Contingency Planning Guidelines Chapter 12 Promotion for further details.

5. How to train people to recognise and then accept there is a contingency?

The decisions on how events might progress through the Life Cycle and move from an Emergency, into a De-Graded Mode of operation and then into a Service Continuity phase will be dependent on the event and its consequences. Supervisors (and managers in certain contexts) have a key role to play here and contingency preparations, execution etc could be included in their OJT/Continuation/Refresher training as appropriate.

3.2 TESTING AND EXERCISING

6. What is the difference between testing and exercising?

Based on the definitions used by the Business Continuity Institute, testing and exercising are described in these Guidelines as follows:

1. Test/Testing is usually associated with a technological procedure and/or business process being tried, perhaps against a target timescale. In this context a piece of equipment could be considered as a 'pass' (i.e. serviceable) or 'fail' (i.e. unserviceable). Examples might be the testing of ground/ground or air/ground communications from an alternate ATM facility in the contingency configuration or check of a call-out cascade system.

2. Exercise/Exercising is normally used for a scenario-based event designed to examine decision-making abilities. An example could be a desk-top exercise to manage a major contingency causing incident.

Note: The BCI also uses the concept of Rehearsing which it describes as the practice of a specific set of procedures, possibly following a script, to build and impart awareness and familiarity. In these Guidelines this is referred to as Training and is covered in 10.2.2 Training for Contingency Modes of Operations.

7. How often should we test and/or exercise our plans for Service Continuity?

There are no mandated timescales for testing and/or exercising.

The need for testing/exercising should therefore be made at a local level and again will be dependent on the measures chosen and in part decided by factors such as built-in redundancy and resilience of existing systems/equipment.

8. Is there a legal requirement to test and/or exercise contingency plans?

There are no mandated requirements from ICAO or the EU in this regard.

However, as a guide, when referring to Aerodrome Emergency Exercises, ICAO Annex 14 states:

" 9.1.12 The plan shall contain procedures for periodic testing of the adequacy of the plan and for reviewing the results in order to improve its effectiveness.

Note. The plan includes all participating agencies and associated equipment.

9.1.13 The plan shall be tested by conducting:

a) a full-scale aerodrome emergency exercise at intervals not exceeding two years; and

b) partial emergency exercises in the intervening year to ensure that any deficiencies found during the full-scale aerodrome emergency exercise have been corrected; and reviewed thereafter, or after an actual emergency, so as to correct any deficiency found during such exercises or actual emergency.

Note. The purpose of a full-scale exercise is to ensure the adequacy of the plan to cope with different types of emergencies. The purpose of a partial exercise is to ensure the adequacy of the response to individual participating agencies and components of the plan, such as the communications system".

9. What are the best mediums to use for testing/exercising contingency plans - drills, tests, exercises, desktop, table-top etc?

There are various means, facilities etc that could be used to test or exercise contingency measures but the choice of which one(s) to choose and how often they should be undertaken is a company/local management decision. The clear aim, however, should be to check the viability of the Contingency Plan(s).

This is not necessarily to test for pass or fail but to examine the overall preparedness of the organisation to respond to a contingency scenario and in particular how the personnel respond.

10. What should be done with lessons learned from testing/exercising?

Sharing lessons learnt whether it is from testing, exercising or a live event is essential and is covered in the Contingency Planning Guidelines, Chapter 12 Promotion .

11. What testing methods should be used and should there be general rules how to test Communication/ Navigation / Surveillance Infrastructure?

Testing methods will be dependent on local needs. If testing is meant to be aimed primarily at equipment systems then clearly the testing regime will depend on the ongoing reliability of equipment (its day-to-day testing/monitoring may suffice), built- in redundancies and overall resilience.

12. Should external suppliers and sub- contractors be involved in training and testing?
What if they fail continually?

The provision of external contractors/suppliers to support contingency plans (including being involved in testing and exercising) should be included in the contracts as appropriate

See also Contingency Planning Guidelines, Appendix G - Systems Engineering Perspective on Contingency Strategies, chapter 2.2
Contractors and Sub-contractors for further details.

13. How do you gauge success/failure without standard requirements?

As stated in the definition [refer Question 6], the testing of equipment is relatively easy to assess. It either works in the contingency configuration or it does not. In terms of exercising, things are slightly more difficult and will depend on the objectives of the exercise which should be clearly stated beforehand.

APPENDIX K - GENERIC SAFETY ARGUMENT FOR CONTINGENCY PLANNING - SERVICE CONTINUITY

1. INTRODUCTION

'Emergency' and 'Degraded' modes of operation are largely covered by current practices, but there is a need to formulate an approach for Service Continuity modes and the transition (Recovery) back to Normal operations.

This Appendix presents a possible methodology, for constructing a Safety Argument to support ANS Contingency Planning - Service Continuity., based on the use of recognised practices such as:

- SAM Title: Air Navigation System Safety Assessment Methodology.
- SCDMTitle: Safety Case Development Manual.
- GS Arg Title: Generic Safety Argument for ATM Safety Assessment.

2. REPRESENTATION OF SERVICE TYPES

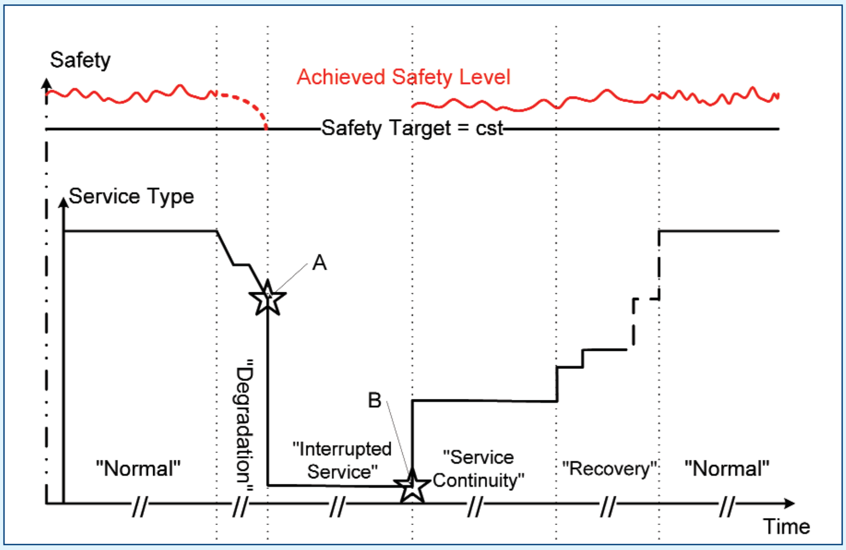


Figure 46: Service Types

This shows the level of safety and the service type in function of the time.

In Figure 46, the horizontal axis shows the time, the durations of the different phases shown are not representative of the length of those phases. They could be very different from one event to another or from one environment to another.

On this figure, 2 vertical axes have been superimposed:

- ***Safety,*** The Safety Target line shows the minimum level of safety that shall be achieved, it is ***not*** a function of time ***nor*** a function of the service type provided.
  The "Achieved Safety Level" represents the level actually achieved by the service provided. It could fluctuate according to certain circumstances or events occurring in the context of the concerned ATM Unit. The "Achieved Safety Level" is considered as "acceptable" as long as it remains above the Safety Target line in Figure 46.
- ***Service Type:*** This represents the evolution from one Mode of Operations (e.g.: "Normal Mode", "Service Continuity Mode"…) to another in function of the time. A Service type/mode of operations should have a defined set of minimum/maximum functionalities, availability of key equipments, key staff etc). Also service types/modes of operations are represented as flat lines: traffic level, staffing, number of sectors operating, availability of some functionalities etc might evolve within a given service type/mode of operations.

Evolution from one mode of operations to another is presented as going from the "Normal Mode of Operations", until a set of failures or shortcomings appear in the system (failure of some equipment, staffing reduced under a given limit, …). Those disruptions could appear all at once or one after another (represented by the dotted stairs).

The key element at this point is for operations personnel (controllers, supervisors, technicians) to identify that during those disruptions, the "Achieved Level of Safety" is degrading. It is very important that a decision is made (before the "achieved level of safety" becoming unacceptable - i.e.: dipping under the safety target-) to change the type of service and to and to go into "Interrupted Service".

In Figure 46, the following is illustrated:

1. Achieved Safety Levels are not easy to

measure, moreover during a phase as dynamic as the "Degradation Phase". The red-dotted line dipping in Figure 46 represents the fact that a decision is needed to switch from the "Normal" to the "Interrupted Service" mode of Operations before the "Achieved Safety Level" becomes unacceptable (i.e.: before it falls below the Safety Target).

2. The Star labelled "A" represents the moment persons in charge of Operations take the decision to go to "Interrupted Service", considering that it is not "safe enough" to keep on working in the current mode of operations.

3. The Star labelled "B" represents the moment the management/political decision is made to go to "Service Continuity". The service continuity mode of operation is fully described by a dedicated operational concept.

In some peculiar circumstances, minimum conditions to go to "Service Continuity" mode of operations might not be met thus requiring the failing Unit to switch to another mode of operations (e.g. into an Emergency mode of operations).

The Service Continuity mode of operation should be fully described by a dedicated operational concept - see Chapter 7.

The "Recovery" phase could be undertaken in one "go" or through a staged approach. It represent the phase where key faulty elements of the system (e.g. equipment, people or procedures) are put back in place (transfer into operation) in order to facilitate the reversion to the "Normal" mode of operations. It is represented as a stepped phase as this is the most generic approach to it.

3. GENERIC SAFETY ARGUMENT OF SERVICE CONTINUITY

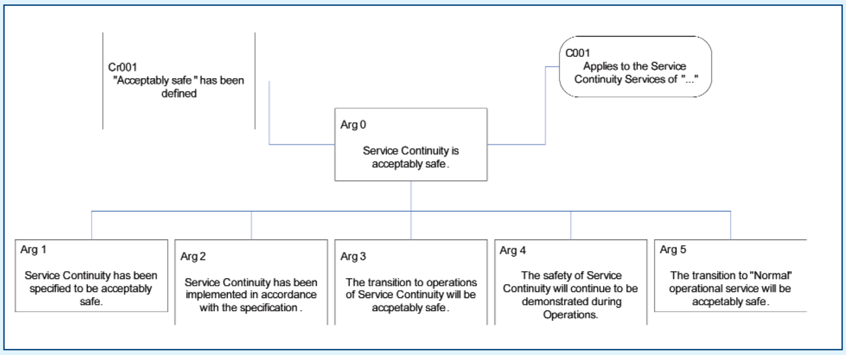

Cr001
"Acceptably safe" has been defined
C001
Applies to the Service Continuity Services of "..."
Arg 0
Service Continuity is acceptably safe.
Arg 1
Service Continuity has been specified to be acceptably safe.
Arg 2
Service Continuity has been implemented in accordance with the specification.
Arg 3
The transition to operations of Service Continuity will be accpetably safe.
Arg 4
The safety of Service Continuity will continue to be demonstrated during Operations.
Arg 5
The transition to "Normal" operational service will be accpetably safe.

Figure 47: Generic Safety Argument for Service Continuity - Arg0.

Figure 47 shows the generic Safety Argument for Service Continuity. This Safety argument is based on Goal Structured Notation (GSN, {SCDM}); where:

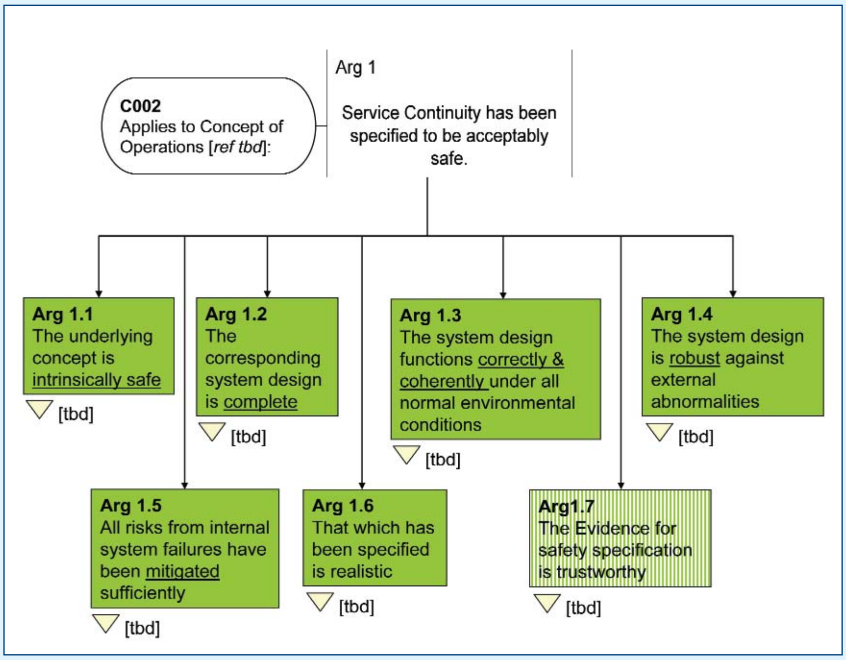
- Cr001 represents the Safety Criteria defining what is "acceptably safe" (this could be an absolute, relative or reductive criteria)
- C001 represents the Context in which the Concept of Service Continuity is considered; i.e.: the operational concept considered in its environment of use (an OPS concept that is considered for one ATS Unit might not be applicable for another one; e.g.: Paris CDG airport vs. a regional airport).
- Arg1 supports the claim that Service Continuity has been specified to be "acceptably safe"
- Arg2 supports the claim that Service Continuity has been implemented to be "acceptably safe"
- Arg3 supports the claim that the transfer into Operations of Service Continuity concept is "acceptably safe". It covers the Safety assessment of the early beginning of the "Service Continuity Phase" shown in Figure 46.
- Arg4 supports the claim that Service Continuity is "acceptably safe" during Operations. It covers the Safety assessment of the operations in "Service Continuity Phase" shown in Figure 46.
- Arg 5 supports the claim that transfer back from Service Continuity to "Normal mode of Operations" is "acceptably safe". It covers the Safety assessment of the "Recovery Phase" shown in Figure 46.

As shown in Figure 47, this Safety Argument is based on the generic Safety Argument presented in {GSArg}. As for any Safety Assessment, it is based on a given Operational Concept that is the baseline of the "Service Continuity" and the related transition phases.

[13] The Safety Assessment of "Service Continuity" is based on the existence of an operational concept. As described in Chapter 7, the Operational Concept for Contingency (which may include "Service Continuity") is the document regrouping all minimum requirements that have to be fulfilled to claim that operations are taking place in the "Service Continuity" mode of operations.

3.1 ARGUMENT - ARG1

Arg1 as shown in Figure 48 is extracted from {GSArg}.



Arg 1
C002
Applies to Concept of Operations [ref tbd]:
Service Continuity has been specified to be acceptably safe.
Arg 1.1
The underlying concept is intrinsically safe
[tbd]
Arg 1.2
The corresponding system design is complete
[tbd]
Arg 1.3
The system design functions correctly & coherently under all normal environmental conditions
[tbd]
Arg 1.4
The system design is robust against external abnormalities
[tbd]
Arg 1.5
All risks from internal system failures have been mitigated sufficiently
[tbd]
Arg 1.6
That which has been specified is realistic
[tbd]
Arg1.7
The Evidence for safety specification is trustworthy
[tbd]

Figure 48: Generic Safety Argument for Service Continuity - Arg1.

INTRINSIC SAFETY OF THE SERVICE CONTINUITY CONCEPT (ARG1.1)

Needs to show, inter alia, that:

- a Functional Model has been clearly described, which completely and correctly interprets the Service Continuity Concept of Operations
- differences from "Normal" operations have been described, in terms of inter alia the Functional Model, understood and reconciled with Safety Criteria
- the impact of the Service Continuity Concept on the operational environment (including interfaces with adjacent systems / airspace) has been assessed and shown to be consistent with the Safety Criteria
- the key (minimum) functionality and performance parameters have been defined and shown to be consistent with the safety criteria.

The issues here are whether the basic idea underlying the Service Continuity Concept has the potential to be safe - ie whether the underlying Concept is capable of satisfying the safety criteria, assuming that a suitable system design could be produced and implemented - and what the minimum parameters are that would enable it to be safe.

DESIGN COMPLETENESS (ARG1.2)

Needs to show that:

- a Logical Model has been clearly described, which completely and correctly interprets the Service Continuity Concept of Operations and Functional Model.
- everything necessary to achieve a safe implementation of the Service Continuity Concept - related to equipment, people, procedures and airspace design - has been specified (as function & performance safety requirements), for each element of the system
- all safety requirements on, and assumptions about, external elements of the end-to-end system have been captured
- Assurance Levels have been correctly assigned to each of the function & performance safety requirements.

The main question here is whether everything has been thought of, in terms of the design that is necessary to fully implement the Service Continuity Concept. Forward and backwards traceability, between the basic Concept/safety criteria and the Safety Requirements, will form a part of the evidence here.

DESIGN CORRECTNESS (ARG1.3)

Needs to show that:

- the system design is internally coherent - eg is consistent in functionality (in equipment, procedures and human tasks), and in use of data, throughout the system
- all reasonably foreseeable normal operational conditions / range of inputs from adjacent systems have been identified

[14] The term 'external' here usually refers to those elements that lie outside the managerial control of the organisation accountable for the safety assessment. However, we don't need to be too rigorous in the distinction between internal and external as long as everything is covered by Arg1.2 and 1.3 as a whole

- the system design is capable of delivering (or maintaining) the required risk reduction under all reasonably foreseeable normal operational conditions / range of inputs
- the system design operates correctly (in accordance with the Concept of Operations) in a dynamic sense, under all reasonably foreseeable normal operational conditions / range of inputs
- the system design operates in a way that is consistent with the operation of adjacent airspace and external systems with which it interfaces / interacts
- the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets.

The main question here is whether the opportunity to reduce risk has been maximised over the full range of conditions that the system is likely to be subjected to in its operational environment.

Note: the Operational concept and the proposed design should provide all details on the minimum set of requirements (including on interfaces) and assumptions that would define the "Service Continuity" mode of operations. In the case of those requirements not being met, the mode of operations would not be "Service Continuity" and the related Safety Case would not apply.

DESIGN ROBUSTNESS (ARG1.4)

Needs to show that:

- the system can react safely to all reasonably foreseeable external failures - ie any failures in its environment / adjacent systems, that are not covered under Arg1.5
- the system can react safely to all other reasonably foreseeable abnormal conditions in its environment / adjacent systems that are not covered under Arg1.3.

Here we the concern is with abnormal conditions in the operational environment, from three perspectives: firstly, can the system continue to operate effectively - i.e. reduce risk?; secondly, if the system cannot continue to operate fully effectively - i.e. its risk-reduction performance is diminished somewhat - is the overall risk still within tolerable limits and can the system recover sufficiently quickly when the abnormality is removed (or at least mitigated)?; and thirdly, to what degree and extent could such abnormal conditions, while they persist, cause the system to behave in a way that could actually induce a risk that would otherwise not have arisen?

MITIGATION OF INTERNAL FAILURES (ARG1.5)

This relates to the more 'traditional' failure-based approach to ATM safety assessment. Unlike Arguments 1.1 to 1.4, which lead to a specification of the risk-reducing properties of the system (ie safety requirements for the functionality and performance of the system), Argument 1.5 leads mainly to a specification of Safety Objectives and Safety Requirements for the integrity of the system.

Typically, it needs to be seen that:

- All reasonably foreseeable hazards, at the boundary of the system, have been identified
- The severity of the effects from each hazard has been correctly assessed, taking account of any mitigations that may be available / could be provided external to the system
- Safety Objectives have been set for each hazard such that the corresponding aggregate risk is within the specified safety criteria
- All reasonably foreseeable causes of each hazard have been identified
- Safety Requirements have been specified (or Assumptions stated) for the causes of each hazard, taking account of any mitigations that are / could be available internal to the system, such that the Safety Objectives (and/or Safety Criteria) are satisfied
- All external and internal mitigations have been captured as either Safety Requirements or Assumptions as appropriate
- A risk assessment for each Hazard has been carried out, and shows that the corresponding aggregate risk is within the specified safety criteria.

Here the concern is with the internal behaviour of the system, from two perspectives: how loss of functionality could reduce the effectiveness of the system in reducing risk?; and how anomalous behaviour of the system could induce a risk that would otherwise not have arisen?

SAFETY REQUIREMENTS VALIDITY (ARG1.6)

Needs to show that:

- All aspects of the system design have been captured as Safety Requirements or (where applicable) as Assumptions

[15] We don't need to be too rigorous in the distinction between normal and abnormal as long as all conditions are covered by Arg1.3 and 1.4 as a whole

[16] Safety Objectives is a term used in ESARR 4 and the EUROCONTROL Safety Assessment Methodology to describe the maximum tolerable occurrence rate of hazards.

- All Safety Requirements are verifiable - ie satisfaction can be demonstrated by direct means (eg testing) or (where applicable) indirectly through appropriate assurance processes (eg HAL, SWAL and PAL)
- All Safety Requirements are capable of being satisfied in a typical implementation in hardware, software, people and procedures.
- All Assumptions have been show to be necessary and valid.

This is a very important issue and continues to be relevant even when Arg2 has been satisfied. The key point is that for Safety Requirements relating to the integrity of software, human tasks, procedures and airspace design, it is very difficult (not to say impossible) to show in a conclusive way that such Safety Requirements have been satisfied in the system implementation. To get around this problem there is the Assurance Level concept which prescribes the rigour of the implementation processes that must be followed according to the criticality (and/or required integrity) of the system element concerned. Since the Evidence from these sources is indirect (equivalent to the legal term "circumstantial") there is a need to support the conclusions regarding Safety Requirements satisfaction with Evidence that the Safety Requirements are, at least, capable of been satisfied.

SAFETY REQUIREMENTS VERIFICATION (ARG1.7)

For each of Arg1.1 to 1.6, need to provide Backing Evidence to show that the (Direct) Evidence supporting these 6 Arguments (including any further decomposition thereof) is trustworthy.

This would normally be done from two perspectives: the processes, tools and techniques used; and the competence of the personnel using them.

3.2 ARGUMENT - ARG2

All details on Arg2 as shown in Figure 49: Generic Safety Argument for Service Continuity - Arg2. are provided in {SCDM}; it supports the claim that "Service Continuity" has been implemented in accordance with the specification.

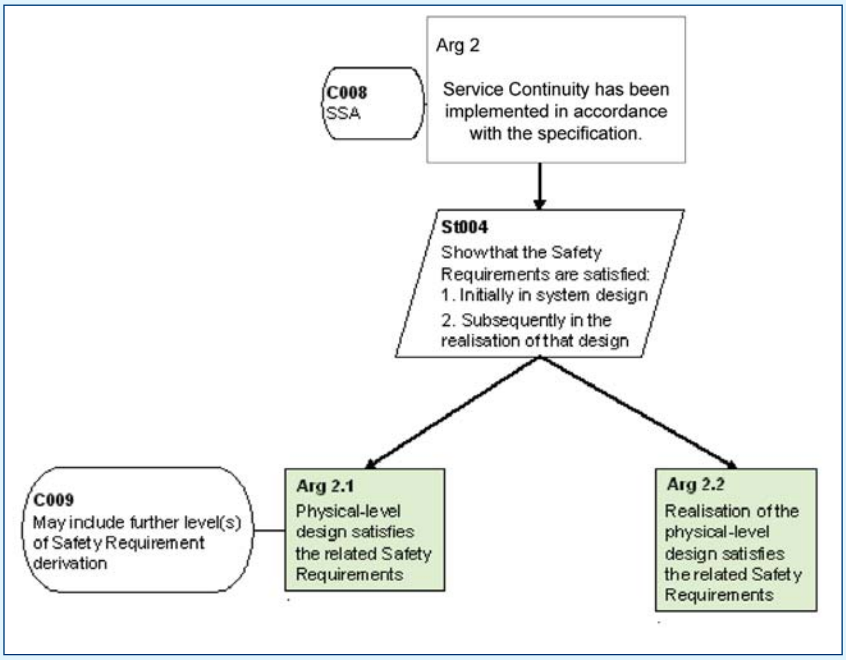

Arg 2
Service Continuity has been implemented in accordance with the specification.
C008
SSA
St004
Show that the Safety Requirements are satisfied:
1. Initially in system design
2. Subsequently in the realisation of that design
C009
May include further level(s) of Safety Requirement derivation
Arg 2.1
Physical-level design satisfies the related Safety Requirements
Arg 2.2
Realisation of the physical-level design satisfies the related Safety Requirements

Figure 49: Generic Safety Argument for Service Continuity - Arg2.

3.3 ARGUMENT - ARG3

Arg3 represent the dedicated safety assessment for the transition phase to "Service Continuity". This means that a plan for transfer into "Service Continuity" is available, i.e. it means that the different credible scenarios that could lead from "normal" to "Service Continuity" mode have been identified and captured/formalised.

One of the demands of going to "Service Continuity" mode of operations might be that the transfer needs to be undertaken quickly. In order to achieve this, the main scenarios that could lead to the need for switching to "Service Continuity" should have been identified and assessed in advance. This would result, at the moment of the switch, in just the need to complete checklists identifying which scenario is underway, what the key elements of that scenario are and making sure that those key elements/requirements are met.

In order to ensure that the transition to Service Continuity operations remains "acceptably safe" (as presented in Figure 46), key indicators defining the different modes of operations need to be identified and monitored. As degradation occurs in the system, appropriate personnel should make decision, based on the evolution of those indicators, to go to "Service Continuity" operation in due time (i.e. before the "Achieved Level of Safety" goes below the Safety Target).

Identifying (thus assessing) all scenarios is very difficult; both in terms of completeness and in terms of resource/time needed. A way forward, would be to identify the key parameters differentiating the credible scenarios and to perform a Safety Assessment of "generic" credible scenarios (see Edition 1.0 of the EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services).

Figure 50 presents a generic approach to Arg3. Its objective is to ensure that risk during and immediately following transition to "Service Continuity" services meets the safety criteria.

As this "Emergency" phase is unexpected, the concept of this transition should be clear and simple. When the decision is made to switch to "Service Continuity", checklists should be available to provide assurance that all pieces of the Service Continuity concept of Operations are in place, i.e.:

- Equipment is ready to be used (it has been verified and validated in the related context).
- Procedures (Ops working methods, technical and maintenance) exist, have been published and are available to related personnel.
- People have been trained for their actions, activities and responsibilities in relation with the concept of Operations defined for "Service Continuity".

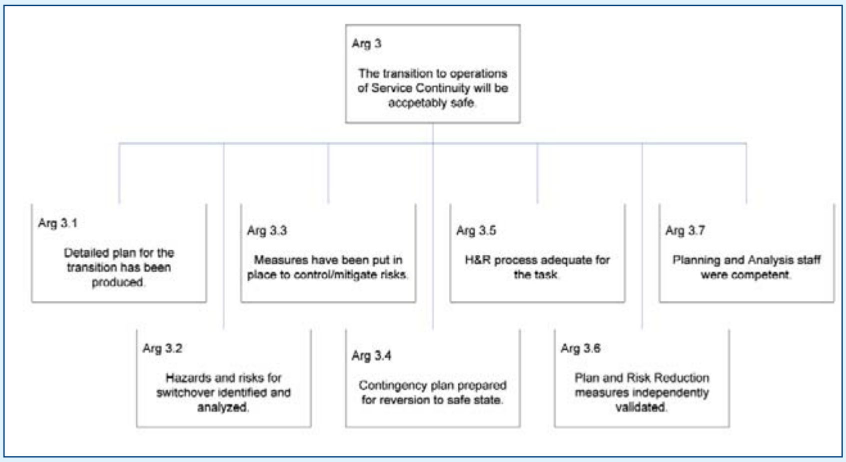

Arg 3
The transition to operations of Service Continuity will be accpetably safe.
Arg 3.1
Detailed plan for the transition has been produced.
Arg 3.3
Measures have been put in place to control/mitigate risks.
Arg 3.5
H&R process adequate for the task.
Arg 3.7
Planning and Analysis staff were competent.
Arg 3.2
Hazards and risks for switchover identified and analyzed.
Arg 3.4
Contingency plan prepared for reversion to safe state.
Arg 3.6
Plan and Risk Reduction measures independently validated.

Figure 50: Generic Safety Argument for Service Continuity - Arg3

Arg3.5, Arg3.6 and Arg3.7 are backing evidence demonstrating that transition into "Service Continuity" direct evidence (i.e.: Arg3.1, Arg3.2, Arg3.3 and Arg3.4) is trustworthy.

As this phase represents an unexpected tactical change (see SAM Part IV, Guidance Material H) to the system, an occurrence report, iaw ESARR 2, should be triggered (and investigated).

3.4 ARGUMENT - ARG4

All details on Arg4 as shown in Figure 51 are provided in {SCDM}, it supports the claim that the safety of "Service Continuity" will continue to be demonstrated during operations.

3.5 ARGUMENT - ARG5

Arg5 represents the dedicated safety assessment for the transition phase back to "Normal" ops. The proposed plan for this transition is function of the Service Continuity mode.This transition plan shall be safety assessed.

Figure 52 presents the Arg5 supporting the claim that risk during and immediately following transition form "Service Continuity" to "Normal" services meets the safety criteria

Arg5.5, Arg5.6 and Arg5.7 are backing evidence demonstrating that transition into "Service Continuity" direct evidence (i.e.: Arg5.1, Arg5.2, Arg5.3 and Arg5.4) is trustworthy.

This transition phase of "Recovery" could be planned for as operations are going from the Service Continuity which is as much as possible a stable state of the system to "Normal mode of Operations" which is another stable state of operations. The "Recovery" phase could be a "big bang" or a stepped approach. It requires none the less, involvement of all actors (including. the NSA/Regulator).

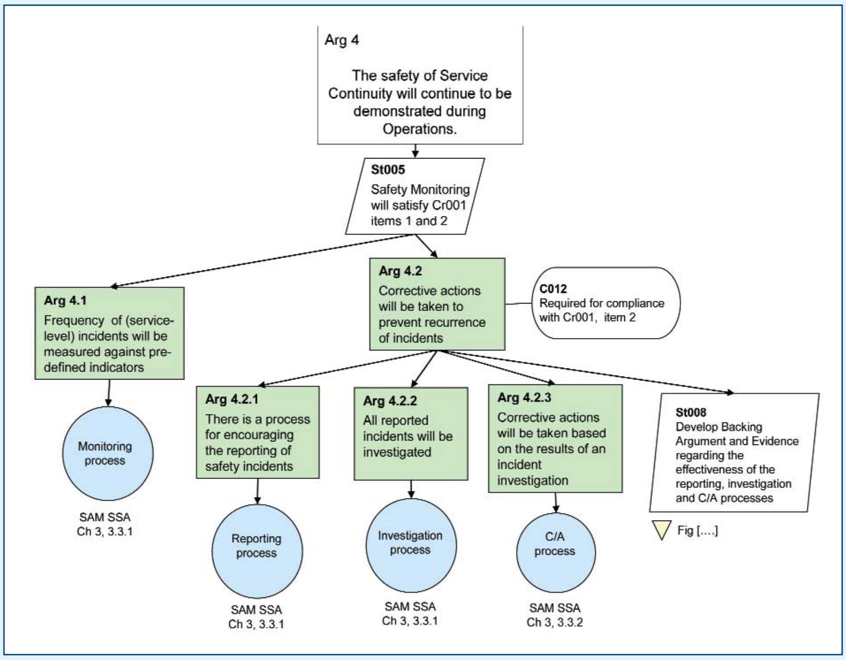

Arg 4
The safety of Service Continuity will continue to be demonstrated during Operations.
St005
Safety Monitoring will satisfy Cr001 items 1 and 2
Arg 4.1
Frequency of (service-level) incidents will be measured against pre-defined indicators
Arg 4.2
Corrective actions will be taken to prevent recurrence of incidents
C012
Required for compliance with Cr001, item 2
Monitoring process
SAM SSA Ch 3, 3.3.1
Arg 4.2.1
There is a process for encouraging the reporting of safety incidents
Arg 4.2.2
All reported incidents will be investigated
Arg 4.2.3
Corrective actions will be taken based on the results of an incident investigation
St008
Develop Backing Argument and Evidence regarding the effectiveness of the reporting, investigation and C/A processes
Fig [....]
Reporting process
SAM SSA Ch 3, 3.3.1
Investigation process
SAM SSA Ch 3, 3.3.1
C/A process
SAM SSA Ch 3, 3.3.2

Figure 51: Generic Safety Argument for Service Continuity - Arg4.

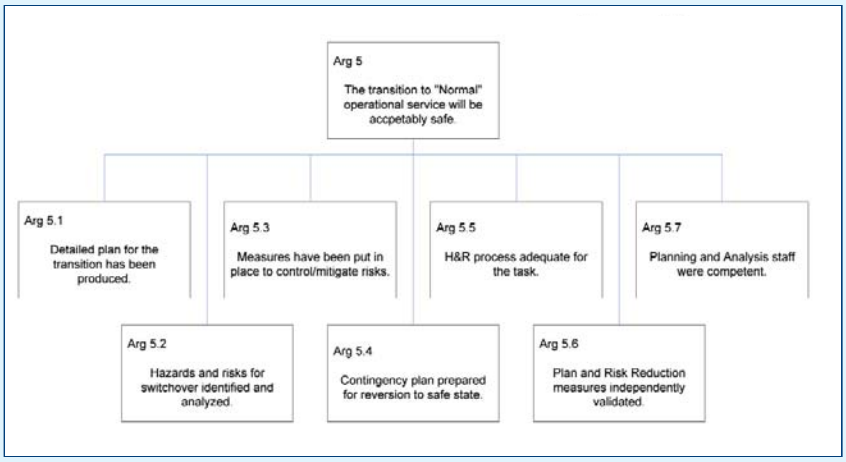

Arg 5
The transition to "Normal" operational service will be accpetably safe.
Arg 5.1
Detailed plan for the transition has been produced.
Arg 5.3
Measures have been put in place to control/mitigate risks.
Arg 5.5
H&R process adequate for the task.
Arg 5.7
Planning and Analysis staff were competent.
Arg 5.2
Hazards and risks for switchover identified and analyzed.
Arg 5.4
Contingency plan prepared for reversion to safe state.
Arg 5.6
Plan and Risk Reduction measures independently validated.

Figure 52: Generic Safety Argument for Service Continuity - Arg5.

4. COMPARISON TO A "GENERIC SAFETY ARGUMENT" FOR NORMAL OPS

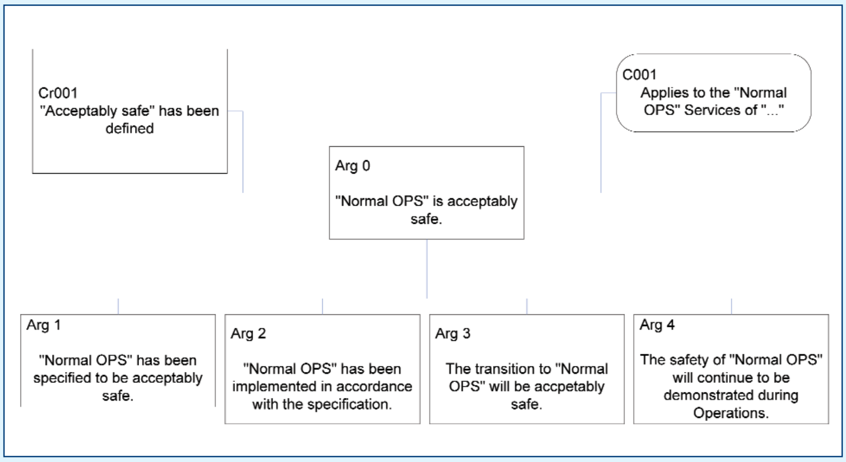

Cr001
"Acceptably safe" has been defined
C001
Applies to the "Normal OPS" Services of "..."
Arg 0
"Normal OPS" is acceptably safe.
Arg 1
"Normal OPS" has been specified to be acceptably safe.
Arg 2
"Normal OPS" has been implemented in accordance with the specification.
Arg 3
The transition to "Normal OPS" will be accpetably safe.
Arg 4
The safety of "Normal OPS" will continue to be demonstrated during Operations.

Figure 53: Generic Safety Argument for "Normal OPS"

When comparing Figure 47: Generic Safety Argument for Service Continuity - Arg0. and Figure 53: Generic Safety Argument for "Normal OPS", it is obvious that they are very similar.

The differences in terms of safety assurance are mainly in:

- "Service Continuity" Arg3 which has no equivalent in the "Generic Safety Argument for Normal OPS";
- "Service Continuity" Arg5 which is almost the same as Normal OPS Arg3;

Regarding the other arguments, only the operational concepts are different between "Normal Operations" and "Service Continuity", the objectives and activities to undertake as assurance/demonstration are the same (for more guidance, see {SCDM} and {SAM}).

5. CONCLUSION

The Safety Assessment of "Service Continuity" should be the same type of Safety Assessment as the one performed for the "Normal Operations" (based on a dedicated Concept of Operations). Likewise, the Safety Assessment of the "Recovery" phase is a Safety Assessment of a transfer into operation phase.

Building a Safety Argument for "Service Continuity" is very similar to the one needed for "Normal Ops" (if not yet included in the Normal Ops operational concept). It relies heavily on the need for a dedicated Operational Concept that describes the different failing scenarios, and if not the scenarios themselves, at least the key parameters (what is the minimum set of the staff, equipment and procedures required to go to "Service Continuity") that, when degraded, will lead to the need for "Service Continuity".

ANSPs should monitor (as part of their SMS/SMM) key indicators including the ones that will allow relevant people in the organisation to make the decision that safety is severely impaired and that it is time to switch to another mode of operations, e.g."Service Continuity".

APPENDIX L - SAFETY AND SECURITY TERMINOLOGY RELATED TO ATM CONTINGENCY PLANNING

The table below describes a number of terms that are common to Safety and Security and which are also used in the context of ATM Contingency Planning. Source References are also included.

TERM	MEANING
Asset	Anything that has value to the organization. Any item of ATM infrastructure, intangible assets also include the reputation of an ANSP. *Source: Sec MS Handbook*
ATM Security	ATM security is concerned with those threats that are aimed at the ATM System directly, such as attacks on ATM assets, or where ATM plays a key role in the prevention or response to threats aimed at other parts of the aviation system (or national and international assets of high value) and limiting their effects on the overall ATM Network. ATM Security is a subset of Aviation Security which is itself a component of Transport Security. *Source: Sec MS Handbook*
Business Continuity	Process involved in ensuring continued service provision, typically after first 48 hours following any contingency. Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level. *Source: Sec MS Handbook*
Business impact analysis (BIA)	Process of analysing business functions and the effect that a business disruption might have upon them. *Source: Sec MS Handbook*
Control	(Countermeasure) An action, device, procedure, or technique that reduces a risk by eliminating or preventing the threat, by minimizing the impact it can cause, or by discovering and reporting it so that corrective action can be taken. In ICT standards, controls include all actions or processes intended to reduce risk, including management, policy, organisation and operation. *Source: Sec ICT*
Failure	The inability of any element of the Air Traffic Management System to perform its intended function or to perform it correctly within specified limits. *Source: ESARR 4*
Hazard	The term "hazard" refers to any issue or condition that either on its own or in combination with others has the potential to create a safety concern. *Source: ESARR 4*
Incident Management Plan	Clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process. *Source: Sec MS Handbook*
Impact	(Threat Consequence, Severity Level) The unwanted consequence of a security incident; the impact may be qualified in financial, opportunity, efficiency, safety or any other relevant business or ATM operational terms. *Source: Sec ICT*
Information Security	Preservation of confidentiality, integrity and availability of information. Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. *Source: Sec MS Handbook*

TERM	MEANING
Likelihood	The chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or mathematical probabilities. *Source: Sec MS Handbook*
Mitigation ***(or risk mitigation)***	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level. *Source: ESARR 3*
Occurrences	Accidents, serious incidents and incidents as well as other defects or malfunctioning of an aircraft, its equipment and any element of the Air Navigation System which is used or intended to be used for the purpose or in connection with the operation of an aircraft or with the provision of an air traffic management service or navigational aid to an aircraft. *Source: ESARR 3*
Resilience	The ability of an organization to resist being affected by an incident. *Source: Sec MS Handbook*
Risk	The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect. *Source: ESARR 3 & 4*
Risk Analysis	Systematic use of information to identify sources and to estimate the risk. *Source: Sec MS Handbook*
Risk Assessment	The overall process of risk identification, analysis and evaluation. *Source: Sec MS Handbook*
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk. *Source: Sec MS Handbook*
Risk Level	A single metric that expresses the overall risk of a particular threat. The risk elements of impact and frequency are often combined into a single metric in way that is justifiable in business terms; this allows the risks to a system to be ranked by sensitivity. *Source: Sec ICT*
Risk Management	The structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling risks. *Source: Sec MS Handbook*
Safety Case	A safety case is an analysis presenting an overall justification for the declaration that a particular system satisfies its safety requirements. *Source: EATM Glossary*
Safety Management Function	A managerial function with organisational responsibility for development and maintenance of an effective safety management system. *Source: ESARR 3*

TERM	MEANING
Safety Management	The management of activities to secure high standards of safety performance which meet, as a minimum, the provisions of safety regulatory requirements. *Source: ESARR 3*
Safety Management System (SMS)	A systematic and explicit approach defining the activities by which safety management is under taken by an organisation in order to achieve acceptable or tolerable safety. *Source: ESARR 3*
Safety Monitoring	A systematic action conducted to detect changes affecting the ATM System with the specific objective of identifying that acceptable or tolerable safety can be met. *Source: ESARR 3*
Safety Policy	A statement of the organisation's fundamental approach to achieve acceptable or tolerable safety. *Source: ESARR 3*
Safety Requirement	A risk mitigation means, defined from the risk mitigation strategy that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics. *Source: ESARR 4*
Security Management	The purpose of security management is to support the application of security policies by means of functions which include the creation, deletion and control of security services and mechanisms, the distribution of security-relevant information and the reporting of security-related events. *Source: EATM Glossary*
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization. It is a function of intention and capability. *Source: Sec MS Handbook*
Threat Agent	Adversary, Attacker, Threat Source) The source of a threat; may be a person, entity, or event, with or without malicious intent. *Source: Sec ICT*
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats. *Source: Sec MS Handbook*

SOURCE REFERENCES:

- EATM Glossary of Terms, available on: http://www.eurocontrol.int/eatm/gallery/content/public/library/terms.pdf
- EUROCONTROL Security Management System (SecMS) Handbook: A Framework. Edition 1.0, May 2008. (available on request)
- ESARR 3, http://www.eurocontrol.int/src/public/standard_page/esarr3.html
- ESARR4, http://www.eurocontrol.int/src/public/standard_page/esarr4.html
- EUROCONTROL Contingency Planning Guidelines for ANS, http://www.eurocontrol.int/ses/public/standard_page/sk_sesis_guidelines.html
- EUROCONTROL ICT Security Guidance (Available on request)

APPENDIX M - ACRONYMS

ACRONYM	DEFINITION
ACC	Area Control Centre
AD	Air Defence
AFTN	Aeronautical Fixed Telecommunications Network
AIC	Aeronautical Information Circular
AIP	Aeronautical Information Publication
AIS	Aeronautical Information Service
AMHS	Automatic Message Handling System
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOP	Airport Operator
AoR	Area of Responsibility
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	Contingency FL Allocation Scheme
CFMU	Central Flow Management Unit
CIA	Contingency Impact Assessment
CIDIN	Common ICAO Data Interchange Network
CM	Crisis Management
CMG	Crisis Management Group
CND	Cooperative Network Design
CNS	Communication, Navigation and Surveillance
CR	Common Requirements
CRAM	Conditional Route Allocation Message
CTF	Contingency Task Force
CTZ	Control Zone
EAB	EAD and Aeronautical Information Bureau (EAB)
EAD	European Aeronautical Information Database
EAM	ESARR Advisory Material
EATCHIP	European Air Traffic Control Harmonisation and Implementation Programme
EATMP	European Air Traffic Management Programme
EC	European Community
ECAA	European Common Aviation Area
ECAC	European Civil Aviation Conference

ACRONYM	DEFINITION
ECIP	European Convergence and Implementation Programme
EEC	EUROCONTROL Experimental Centre
EDD	Electronic Data Display
ESARR	EUROCONTROL Safety Regulatory Requirement
ESP	European Safety Programme for ATM
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAB	Functional Airspace Block
FDM	Flight Data Management
FDP	Flight Data Processing
FIR	Flight Information Region
FL	Flight Level
FPL	Flight Plan
FUA	Flexible Use of Airspace
GAT	General Air Traffic
HMI	Human Machine Interface
HR	Human Resources
IA	Impact assessment
ICAO	International Civil Aviation Organisation
LoA	Letter of Agreement
MET	Meteorological
MoT	Ministry of Transport
MoU	Memorandum of Understanding
MAPD	Maximum Agreed Period of Disruption
NOTAM	Notice to Airmen
NATO	North Atlantic Treaty Organisation
NEASCOG	NATO-EUROCONTROL Airspace Security Coordinating Group
NSA	National Supervisory Authority
OAT	Operational Air Traffic
OCG	Operational Coordination Group
ODS	Operational Display
OLDI	On Line Data Interchange
OPMET	Operational Meteorological (Information)
PAL	Procedure Assurance Level
RA	Risk Assessment
RE	Realistic Event
R&D	Research and Development
RVSM	Reduced Vertical Separation Minima
SAM	Safety Assessment Methodology
SAAP	Safety Assessment of ATM Procedure
SES	Single European Sky
SESAR	Single European Sky ATM Research
SecMS	Security Management System
SID	Standard Instrument Departure

ACRONYM	DEFINITION
SM	Safety Management
SMS	Safety Management System
SPIN	Safety Nets Planning Implementation & Enhancement
SRC	Safety Regulation Commission
SSH	Safety, Security, Human Factors Division
STAR	Standard Arrival Route
TAF	Terminal Area (Aerodrome) Forecast
TDU	Training Development Unit
TIBA	Traffic Information Broadcasts by Aircraft
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
TWR	Tower (ATC)
UAC	Upper Area Control Centre
UIR	Upper Information Region
VCS	Voice Communication System
WAFC	World Area Forecast Centre

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 "Reference Guide to EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services (including Service Continuity)" that may also be obtained from the EUROCONTROL Internet or E-mail addresses listed above.

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

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