# High-Level Architectures for Contingency Planning in Air Traffic Management

Chris. W. Johnson, DPhil;
Department of Computing Science, University of Glasgow, Scotland, UK.

Gerald Amar, Tony Licu and Richard Lawrence,
EUROCONTROL, Safety Security and Human Factors Division, Rue de la Fusée, 96, 1130 Brussels, Belgium.

Keywords: Air Traffic Management; Contingency Planning; Pandemics; Recovery.

## Abstract

Over the last eighteen months, a project team from the European Organization for the Safety of Air Navigation has worked with a task force drawn from regulators and Air Navigation Service Providers (ANSPs) to draft guidelines for contingency planning. The intention is to help Air Traffic Management (ATM) organisations prepare for the potential loss of a major unit following possible scenarios that include but are not limited to systems failure, terrorist actions, floods, fires and pandemics. As part of this work, a study was conducted to identify current and best practice in contingency planning. This paper provides a brief introduction to the different architectures that were identified. The intention is to help service providers identify the different ways in which they can prepare resources for a wide range of threats to key components of national safety-critical infrastructures.

## Introduction

The events of 2001 and subsequent attacks on London and Madrid have revealed new dimensions to the threats that exist for national critical infrastructures. The response to hurricane Katrina and the realization that we face significant climate change have raised concerns across a range of safety-critical industries. Partly in response, the European Commission requires that Air Navigation Service Providers (ANSPs) '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'. This paper presents different ways that ANSPs can structure contingency provision by developing co-located contingency facilities; multi-use facilities; centralized facilities; common system solutions; ATS delegation and hybrid models. Each of these different architectures was identified following site visits to a number of European and North American service providers. Although our focus is on Air Traffic Management, many of these distinctions are applicable to contingency planning across a range of other industries.

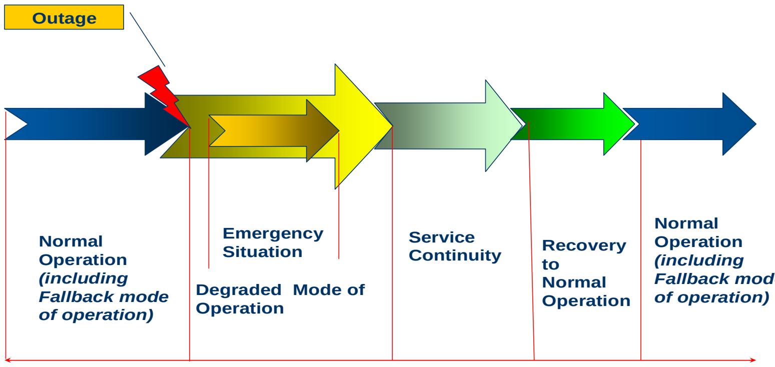
Outage
Normal Operation (including Fallback mode of operation)
Emergency Situation
Degraded Mode of Operation
Service Continuity
Recovery to Normal Operation
Normal Operation (including Fallback mode of operation)

**Figure 1: Generic Contingency Life-Cycle**

Figure 1 provides a high level view of five different stages in the contingency 'life cycle'. For example, a Degraded Mode of Operation might be resolved before an emergency can develop and hence would lead directly to Recovery and Normal Operations. Similarly, in some situations, it might be necessary to move straight from 'Normal Operation' into 'Service Continuity'. This high-level model provides a structure or framework for the more detailed plans that each service provider must develop within their local context of operation.

| **Planning & Maintenance** |
|---|
| **Phase 1 – Preparation of Plans** |
| • Establish contingency planning group including preliminary consultation with airspace users and the airports.<br>• Document contingency plans.<br>• Identify key resources including facilities management. |
| **Phase 2 - Maintenance of Plans** |
| • Update contingency plans to reflect changes in systems, procedures and operating environment.<br>• Develop and implement drills/tabletop exercises to assess adequacy of plans for different scenarios. |
| **Fail to safe** |
| **Phase 3 - Immediate Actions** |
| • A dangerous situation has been identified;<br>• the actual traffic situation shall be secured.<br>• may be difficult to determine magnitude of problem and the duration of the outage.<br>• Must prepare fall-back instructions to ensure the safety of operations allowing a 'smooth' transition to following phases.<br>• Appropriate authorities will identify the seriousness of the situation and initiate appropriate contingency measures. |
| **Phase 4: Short/Medium Term Actions (<48 hours)** |
| Focuses on the safe handling of aircraft in the airspace of the failing unit, using all technical means still operationally available.<br>• Evacuation of the airspace;<br>• contingency measures shall be initiated;<br>• notification of all concerned,<br>• determination and coordination of flow control measures;<br>• delegation of ATS will be initiated where appropriate. |
| **Service Continuity** |
| **Phase 5: Relocation:** |
| Starts when staff of the failing unit arrive at the aiding unit(s).<br>• detachment of staff to the aiding unit(s);<br>• opening of contingency working positions at aiding unit(s);<br>• stabilization of new situation;<br>• improving the flow capacity.<br>• ICAO route structure and sectorisation in failing unit shall remain unchanged.<br>• all technical means shall be made available to establish and maintain communication necessary to provide ATS in the failing unit. |
| **Phase 6: Optimisation** |
| • Staff of the failing unit should become familiar with the operational facilities of the aiding unit. The aim is to optimize capacity with the available resources within the published ICAO route and sectorisation structures.<br>• Means of communication should be upgraded as much as is possible.<br>• Coordination procedures should revert back to 'normal' handling. |
| **Recovery** |
| **Phase 7: Longer-term Response and Debrief** |
| o Revert back to the original unit and working position; Coordinate the start of normal operations.<br>o A Transition plan shall be started taking into account technical and operational conditions. As soon as the failing unit has decided to revert back to the original facilities, the appropriate authority of that unit shall inform all partners.<br>o The failing unit must co-ordinate the time at which normal operations can be resumed.<br>o Updates must be implemented to flight plan and radar data processing systems. |

**Figure 2: Generic Overview of the Key Phases in the Execution of Contingency Plans**

Figure 2 summarises builds on the life cycle in Figure 1 to identify a number of more detailed concerns that arise during the development of contingency plans and the response to any major incident. The intention is to provide a generic template that Air Navigation Service Providers (ANSPs) can build on when they develop local plans that are tailored to their operating environment and characteristics. A number of site visits were organised to Air Navigation Service Providers (ANSPs) in Europe and in North America to validate this initial work. A range of different plans were identified. For example, some service providers were sceptical about their neighbours' ability to meet the complex demands of their national traffic patterns. They, therefore, built a specialist national facility that is intended to provide fallback support for all of their major centres. The following pages describe the different approaches in greater detail.

## International Delegation of Air Traffic Services

International agreements, such as the International Civil Aviation Organisations Annex 11, assume that ANSPs will not intervene to control the national airspace of another service provider, except when there are agreements on cross-border areas. Most of these international arrangements are drafted for operational reasons; very few specifically enable nations to help their neighbours recover from terrorist attacks or major infrastructure failures. International letters of agreement provide a flexible and cost effective approach to contingency planning. However, they require technical and political agreement. Such consensus can be difficult if there is any perception that control will be surrendered for some portion of national airspace.

During initial planning and maintenance (Phases 1 and 2) it is important to establish lists of contacts and telephone numbers so that key personnel in each ANSP can communicate at short notice. This might seem like an obvious requirement. However, the site visits revealed incidents in which operational staff could not contact their colleagues in another centre because calls from outside their unit were diverted through the general switchboard and could not be re-routed to the control room. During Phase 3, neighbouring units must be alerted to the potential for a contingency. In Phase 4, 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. Phase 5 focuses on the relocation of ATM services. In most letters of agreement, it is not possible to exchange operational staff. Different national regulatory frameworks, different Standard Operating Procedures and technical infrastructures all complicate the relocation of operational staff. However, it may be necessary for management and systems engineers to relocate in support of an aiding unit. During phase 6, ANSPs can begin to optimise continued service provision from contingency facilities. This phase builds on the initial route structures and policies that must be put in place before a contingency occurs. For example, it will be important to consider knock-on consequences or on third-party states that will be affected by the increase in workload for the aiding units. These knock-on effects are a consequence of increasing integration across safety-critical infrastructures. Phase 7 of the contingency lifecycle must feedback any lessons learned into the planning process. It may consider revisions to letters of agreement and to the technical or managerial annexes, especially in the light of impact studies and risk assessments for third parties affected by ‘knock-on’ workload during a contingency.

| **Planning & Maintenance** |
|---|
| **Phase 1 - Preparation of Plans Additional requirements for ATS Delegation**<br>**(International Letters of Agreement - LoA)** |
| • Establish political and regulatory support for ATS Delegation approach supported by LoAs; identify technical extent of any support.<br>• Develop list of contacts and shared procedures. |
| **Phase 2 – Maintenance of Plans** |
| • Practice hand-overs under contingency to neighbouring units and update LoAs after changes in operating environment or procedures.<br>• Ensure exchange of best practice between neighbouring states following drills, table-top exercises etc. |
| **Fail to Safe** |
| **Phase 3 – Immediate Actions** |
| • During this phase, all neighbouring units must be alerted under conditions in letters of agreement and political support may be necessary.<br>• The aiding unit must confirm initial report from failing unit and secure political/managerial approval for response.<br>• Decisions must be taken on whether to close the skies or to allow some services to continue while situation is being assessed.<br>• May be necessary to alert other agencies including CFMU of potential contingency and changes in regional traffic between neighbouring states. |
| **Phase 4 – Short/Medium Term Actions (<48 hours)** |
| • Begin hand-over from failing unit to neighbouring states facilities, OPS in failing unit must verify that all aircraft are accounted for.<br>• OPS in failing unit must also consider residual services to military and government aircraft that may be maintained even under immediate decision to clear the skies.<br>• More detailed discussions will be needed with neighbours about medium term flow control. |
| **Service Continuity** |
| **Phase 5 - Relocation** |
| • Sectorisation changes may be needed if neighbours cannot replicate facilities and coverage of failing unit.<br>• Key management staff and regulatory officials may move to aiding state to ease communication and support response to contingency.<br>• SYS teams focus on diagnosis of problem and remedial actions to restore failing unit and ease load on neighbouring ANSP. |
| **Phase 6 - Optimisation of ATS Delegation** |
| • Any residual capacity in the failing unit must be allocated – eg to emergency flights.<br>• Some of the load on neighbouring ANSPs might be taken on by other regional units in the ANSP operating the failed unit. |
| **Recovery** |
| **Phase 7 - Longer-term response and Debrief** |
| • Bring the failed unit back to operational readiness.<br>• Identify protocol and timescale for handing back to failed unit.<br>• After recovery hold debrief and redraft letter of agreement or the technical annex as necessary.<br>• Review impact of contingency plans on regional units in both states and third parties in terms of safety, security and performance. |

**Figure 3:** Characteristics of International Delegation of Air Traffic Services for Contingency Planning

## Co-Located Facilities

Many of the ANSPs that we visited have created contingency resources on the same site as their primary centres. To further reduce costs, they also share the hardware that might be used during any failure with simulation and development facilities. The workstations, processors and local area networks that are usually available to help train air traffic controllers can be converted to full operational use if the primary systems are threatened by a potential contingency. This helps to ensure that secondary control rooms do not remain empty during long periods of normal operation. However, this approach has limitations. Some scenarios, such as floods, earthquakes or terrorist attacks, could affect primary and contingency resources if they are on the same site. However, not all dual use facilities are co-located. Some ANSPs propose the development of national centres on their training Academy sites a short distance away from major national control centres. During the initial phases of any contingency it may be possible for staff to begin the configuration of a co-located facility to take over from the primary system. Depending on the extent of this task, contingent systems can also be used to assist in 'clearing the skies'. During Phase 3 management support may be required to confirm the dedicated use of shared, co-located facilities by contingency groups. It is important during Phase 4 that systems teams validate both the technical infrastructure and also the data that is used to configure contingency systems. Optimisation and recovery phases (6 and 7) can be aided by the development of training resources beyond those that are needed in the contingency response so that watches ideally have an opportunity to rehearse the hand-over and flow regulation as primary systems come back on-line. These observations are summarised in Figure 4.

| **Planning & Maintenance** |
|---|
| **Phase 1 Preparation of Plans, Additional Requirements for Co-Located Facilities** |
| • Establish co-located facility. |
| **Phase 2 – Maintenance of Plans** |
| • If necessary, establish agreements with dual use groups for training time and for access conditions to rehearse contingency plans. |
| **Fail to Safe** |
| **Phase 3: Immediate Actions** |
| • During this phase dual users of a co-located facility must be informed of a potential incident.<br>• Management permission needed to requisition shared resources, initial steps may be taken to reconfigure the co-located facility.<br>• Initial steps can be taken to prepare for contingency facility use in clearing the skies if a 'hot swap' is possible.<br>• Consider contingencies involving contingency facility. |
| **Phase 4: Short/medium Term Actions (<48 hours)** |
| • Complete configuration of co-located facilities.<br>• Initiate contingency for security/facilities management etc at co-located site<br>• 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.<br>• Depending on contingency plan for gradual hand-over to co-located Facility. |
| **Service Continuity** |
| **Phase 5: Relocation:** |
| • Relocation should be minor in terms of physical move to adjoining site.<br>• Sectorisation changes may be needed if the co-located facilities have less positions/resources than primary site.<br>• Systems team validate safety of data and communications infrastructure as co-located facility goes live and during initial operation.<br>• Secure lines of command and management by only allowing necessary staff to remain on-site. |
| **Phase 6: Optimisation at Co-located Unit** |
| • Slowly increase capacity up to maximum potential of co-located contingency resource in consultation with end-users and regulators.<br>• Bring in additional staff to ensure adequate rest and rotation of watches/shifts.<br>• Training of additional staff on co-located facility to aid shift rotation etc. |
| **Recovery** |
| **Phase 7: Longer-term Response and Debrief** |
| • Bring the failed unit back to operational readiness.<br>• Carefully assign staff between failed unit and co-located facility in case recovery fails.<br>• Release shared resources, after recovery hold debrief and refine plans for co-located contingency centre. |

**Figure 4:** Characteristics of Co-located Facilities for Contingency Planning

The development of co-located contingency facilities on the same sites as primary centres often involves the redeployment of obsolete systems. These applications can be 'moth-balled' in a way that enables ops teams to use them if the primary system fails. However, this can raise safety concerns given that regulators would have to continue to approve the limited use of previous systems that have been replaced by more modern applications. In some states, contingency facilities are based on paper strips even though these systems have long been phased out of everyday operation. Co-located facilities create a number of further problems for contingency planning. Management teams can be overwhelmed by large numbers of staff wanting to 'lend a hand' in the immediate aftermath of an incident. This can create problems if these staff are needed when the initial watches come off shift. There is also a danger that they will interfere and place additional demands on security and facilities management.

### Multi-Use Facilities (Training Development Units, Training Schools, Simulators)

The costs of contingency provision can be shared by redeploying training and simulation systems when a primary facility fails. These dual-use infrastructures (e.g. training and test suites, simulators etc) may or may not be on the same sites as primary centres. Problems can arise because contingency managers often need access to these shared resources to run exercises and drills; the resource would then not be available for use by other members of an ANSP. Contention for these resources must be considered during initial planning. It is critical that the others users of the shared systems can free the resource when it is required during a contingency. During Phases 3 (Immediate Actions) and 4 (Short and Medium Term Actions) staff must reconfigure the contingency facility away from its normal use as a training or simulation facility so that it can act as a primary system. Phase 4 must also consider facilities management and site access/security as the contingency facility becomes active. Figure 5 provides a brief summary of the principle characteristics of multi-use approaches to contingency planning.

| **Planning & Maintenance** |
|---|
| **Phase 1- Preparation of Plans: Additional Requirements for Multi Use Facilities** |
| • Establish Multi-Use facility, plan for relocation of staff who normally use facility so contingency staff can come in. |
| **Phase 2 - Maintenance of Plans** |
| • Establish agreements with dual use groups for training time and for access conditions under contingency. |
| **Fail to Safe** |
| **Phase 3 – Immediate Actions** |
| • Normal users of shared facility informed of a potential incident, management permission needed to requisition shared resources.<br>• Initial steps to reconfigure facility, prepare to clearing the skies if a 'hot swap' is possible.<br>• Consider contingencies that might affect contingency facility eg further terrorist attack on new site. |
| **Phase 4 - Short/Medium Term Actions (< 48 hours)** |
| • Complete configuration of Multi-Use facilities, ensure security of Multi-Use site<br>• 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. |
| **Service Continuity** |
| **Phase 5 - Relocation** |
| • Relocation should be minor in terms of physical move to adjacent site.<br>• Sectorisation changes may be needed if Multi-Use facilities have less positions/resources than primary site.<br>• Ensure systems team validate reliability of data and communications infrastructure not just as Multi-Use facility goes live but also during initial operation.<br>• Secure lines of command and management by only allowing necessary staff to remain on-site. |
| **Phase 6 - Optimisation at Multi-use Unit** |
| • Gradual increase in capacity up to maximum potential of Multi-Use resource in consultation with end-users and with regulators.<br>• Bring in additional staff to ensure adequate rest and rotation of watches.<br>• Training of additional staff on Multi-Use facility to aid shift rotation etc. |
| **Recovery** |
| **Phase 7 - Longer-term Response and Debrief** |
| • Bring the failed unit back to operational readiness.<br>• Carefully assign staff between failed unit and Multi-Use facility in case recovery fails.<br>• Release shared resources<br>• After recovery hold debrief and refine plans for Multi-Use contingency centre. |

**Figure 5:** Characteristics of Multi-Use Facilities for Contingency Planning

## Centralised (National) Facilities

Single contingency centres can be developed to cover several ATM units. This reduces the costs 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 the other regional sites. Many aspects of the centralised architecture are similar to those described as co-located and multi-use; however, they are not mutually exclusive. For instance, even in a Centralised system it is likely that the national centralised contingency centre will be co-located with at least one ATM centre. The planning process (Phase 1) 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. For example, it makes little sense to develop contingency facilities within an area that is vulnerable to seismic activity.

| **Planning** |
|---|
| **Phase 1 - Preparation of Plans: Additional Requirements for Centralised Facilities** |
| • Establish review of needs across organisation.<br>• Identify location of centralised facility and secure agreements across other units.<br>• Where necessary develop additional marginal resources eg mobile towers? |
| **Phase 2 – Maintenance of Plans** |
| • Establish management processes to ensure updates from outlying units are reflected by changes in centralised facility.<br>• Establish training procedures to ensure that centralised facility can be used to support diverse contingency requirements for all of the sites that share these centralised resources. |
| **Fail to Safe** |
| **Phase 3 – Immediate Actions** |
| • During this phase the other users of a centralised facility must be informed of a potential incident as they may lose backup cover.<br>• Some initial steps may be taken to reconfigure the centralised facility.<br>• Initial steps can be taken to prepare for centralised facility use in clearing the skies if a 'hot swap' is possible.<br>• Consider contingencies involving contingency facility possibly by identifying lead unit for secondary contingency. |
| **Phase 4 – Short/Medium Term Actions (<48 hours)** |
| • Complete configuration of the centralised facilities.<br>• Initiate contingency for security/facilities management etc at the centralised site<br>• Depending on contingency, plan for gradual hand-over to centralised facility (flight plan, radar, communications etc).<br>• Identify key staff to be moved from failing unit and possibly from other eligible units to centralised facility. |
| **Service Continuity** |
| **Phase 5 - Relocation** |
| • Operational and System support staff will be moved – some, however, may already be available at centralised facility.<br>• Sectorisation changes may be needed if centralised facilities have less working positions/resources available than primary site.<br>• Ensure systems team validate reliability of data and communications infrastructure not just as centralised facility goes live but also during initial operation.<br>• Secure lines of command and management by only allowing necessary staff to travel to centralised site.<br>• Rest remain at failing unit to secure recovery. |
| **Phase 6 - Optimisation** |
| • Gradual increase in capacity up to maximum potential of the co-located contingency resource in consultation with end-users and with regulators.<br>• Bring in additional staff to ensure adequate rest and rotation of watches.<br>• Training of additional staff on centralised facility to aid shift rotation etc. |
| **Recovery** |
| **Phase 7- Longer-term Response and Debrief** |
| • Bring the failed unit back to operational readiness.<br>• Carefully assign staff between failed unit and centralised facility in case recovery fails.<br>• After recovery, hold debriefings and refine plans for contingency centre.<br>• Review impact of contingency plans on other units as well as failing centre in terms of safety, security and operational performance. |

**Figure 6:** Characteristics of Centralised Facilities for Contingency Planning

There are further safety concerns over the operation of centralised contingency facilities to cover many regional operations within an Air Navigation Service Provider. It is difficult to ensure that staff in a central contingency facility have sufficient operational experience and competency to fulfil all the roles that must be performed during a wide range of contingency scenarios across many different operational units. There will, therefore, be a need to supplement the contingency facility with decentralised resources including mobile towers. During Phase 3, other users who share the centralised facility must be alerted that a failing unit has made a call upon this scarce resource. Once staff from the failing centre acquire the contingency centre, other centres may not then be able to use it if they suffer similar problems. At this stage, it may be possible to conduct a ‘Hot Swap’ from the failing unit before the ‘skies are cleared’ if the contingency facility is well supported and the configuration issues are relatively straightforward. This needs a high level of training and coordination, which may be possible in a centralised facility within a single national system. Decisions must be made about the best allocation of human resources between the failing and the centralised unit. Staff need to be rested; shifts rotated and training delivered to ensure that operations are optimized in the centralised contingency unit. Feedback in Phase 7 will be particularly important for the future of the centralised facility. Possible shortcomings may raise the political issues that often complicate the establishment of single, centralised facilities as staff in regional centres may question their ability to support them during any adverse event.

Shared Common Systems (International Contingency Centres/Centres in Adjacent States)

The costs of building and maintaining contingency facilities are so great that several ANSPs have suggested sharing a contingency facility between neighbouring countries. This may be a purpose built stand alone facility or an agreement that an existing facility in a nominated state will act as the contingency facility for all participating states. This scenario has not been implemented within European airspace. However, it is important to note shared contingency facilities between States can be seen as a natural development of recent initiatives to implement Functional Airspace Blocks (FABs). This will enable different nations to cooperate in providing common services to airspace users. There are, however, practical drawbacks. It is difficult to ensure that software and staff in the shared centre can be configured to meet the needs of several different nations. Even if countries operate similar technical systems, it will still be necessary to configure the data and sectorisation for any failing unit. Radar and communications infrastructure must be patched to the shared contingency control facility. Flight planning data and other data must also be transferred.

| **Planning & Maintenance** |
|---|
| **Phase 1 - Preparation of Plans: Additional requirements for Shared Common System Facilities** |
| • Establish shared common centre, rnsure centre has software, documentation for each national site to be covered etc.<br>• Arrange for regulatory oversight/approval if staff must move to shared site in another country.<br>• Plan to minimise social ‘disruption’ for staff who may be moved to shared centre for long periods of time. |
| **Phase 2 – Maintenance of Plans** |
| • Establish management processes to ensure shared facilities updated to operational environment of each nation that might use it.<br>• Ensure that each state has adequate training and exercise time on the shared facility so that plans can be revised as necessary.<br>• Ensure that operational experience with shared facility is communicated to all stakeholders in different nations. |
| **‘Fail to Safe’** |
| **Phase 3 – Immediate Actions** |
| • Common centre must be informed of a potential incident, initial steps to reconfigure shared facility.<br>• Other potential end users may be alerted because they will lose their fallback systems if they are shared with the common centre.<br>• Other users of shared common centre may help to ‘clear the skies’. |
| **Phase 4 – Short/Medium term actions (<48 hours)** |
| • It will be hard for any shared common centre to help in clearing the skies unless qualified staff are on-site.<br>• Confirm delegation of responsibility to shared common centre for Phase 3 on at national regulatory level.<br>• Complete configuration of the shared common site for relocation, initiate facilities management at shared common site. |
| **Service Continuity** |
| **Phase 5 - Relocation** |
| • Send operational staff and systems support to shared common centre, change sectors and flow for shared facility.<br>• National regulatory agency or parts of it may need to relocate together with ops and sys teams with support from host regulator.<br>• Predetermined lists used to determine who will remain behind to help in recovery of failed unit. |
| **Phase 6 - Optimisation of Common System** |
| • Gradual increase capacity to maximum potential of shared resource in consultation with end-users and with regulators.<br>• Transfer of additional staff to shared common centre to ensure adequate rest and rotation of watches.<br>• Training of additional staff on shared facility to aid shift rotation etc. |
| **Recovery** |
| **Phase 7 - Longer-term response and Debrief** |
| • Bring failed unit back to operational readiness, inform all users of shared centre both of diagnosis and plan for recovery.<br>• Carefully assign staff between failed unit and shared common facility in case recovery fails.<br>• After recovery hold debrief and refine plans for shared common contingency centre. |

**Figure 7:** Characteristics of Common Systems Solution for Contingency Planning

Further issues complicate the sharing of contingency facilities between states. Ideally there should be minimal differences in the Human Machine Interface between the contingency facility and the failing unit. This enables staff to transfer skills and expertise between facilities. However, individual ANSPs may disagree over the format of the HMI so that the contingency facility may have to be continually updated to support all of the potential end users. Further practical problems stem from the time needed to move people between a primary facility and a shared site in another state. There is a need to obtain approval from regulators and state authority for procedures and practices that affect the airspace of the failing unit. Licensing and training issues must be clarified when staff may be providing safety related services for the airspace of a neighbouring country. There are considerable safety concerns over any attempt to improvise regulatory approval during any contingency. It is, therefore, important that plans are made well before an incident occurs. Service providers must also plan to support staff at a shared facility for prolonged periods of time, for example, if a primary centre cannot easily be brought back. These preparations can include dialogues with unions and other staff representatives so that operational and technical teams understand their potential role during any contingency. It will also be important to consider the transfer of staff back to the failing unit when 'normal operations' are ready to be resumed.

## Hybrid Models

Most ANSPs operate variations on the models that are introduced in this paper, for example, they may distribute limited resources to respond to adverse events in regional units but also retain contingency facilities in a national centre or Training Academy. 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 Letters of Agreement with adjacent states. The same provider was also in negotiation to establish a common centre that would be shared amongst all states that operated similar software. It remains to be seen whether the potential complexity of combining these different approaches will have any impact on the safety of future contingency operations.

## Vulnerable Scenarios

Unfortunately, there are several different contingency scenarios that create particular hazards for all of the approaches identified in previous sections. These include pandemics, software failure and security breaches within an Air Navigation Service Provider or sub-contracting organization.

*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 across a large region. Recent concerns have focused on Severe Acute Respiratory Syndrome (SARS) and the H5N1 strain of the avian influenza virus. Neither has been eradicated, and the World Health Organisation argues that we are in an inter-pandemic period. Figure 8 shows how the five phase model for contingency planning in Air Traffic Management can also be used to structure the response to a pandemic. **There are strong differences between the activities in these plans and those that might be used in other contingencies**. Instead of supporting relocation to aiding units, the aim is to isolate staff and limit movements that might expose them to the risks of infection. It is important also to note that this model is architecture neutral. It could be used along with any of the other models introduced in this paper. For example, if an ANSP had developed a centralised fallback centre for use during other adverse events then staff might be brought in to this unit during a 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.

*Software Bugs:* If the same code is used in a primary system as well as a contingency facility then there is a danger that a single bug could cause both units to fail. This concern would affect co-located systems just as it would regional or national centres. The increasing integration and complexity of ATM systems makes it more and more difficult to identify and diagnose software failures, especially given some of the plans for future airspace configurations in both Europe and North America. A number of techniques can, however, help to address these common mode failures. For instance, N-version programming ensures 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 or incomplete requirements. Other ANSPs use careful version control so that it should always be possible to roll back to a previous working version of a system. This can take a considerable amount of time depending on the point at which any bug was introduced into an application. Previous versions of any code can, therefore, be retained on training and development systems so that they can more easily be restored under contingency.

| **Planning & Maintenance** |
|---|
| **Phase 1 - Preparation of Plans  Additional requirements for Pandemic Contingency** |
| • Establish pandemic management cell.<br>• Establish agreements for systems staff, operational staff and facilities management to move to centre in phases 5 and 6.<br>• Agree plans with regulators and government to ensure ANSPs informed by national contingency committees.<br>• Agree plans for over-flights in pandemic. |
| **Phase 2 – Maintenance of Plans** |
| • Develop management systems to update plans following changes in operational environment, procedures and practices.<br>• Update plans following changes in government, EC and WHO guidance eg over immunisation. |
| **Fail to Safe** |
| **Phase 3:  Immediate Actions** |
| • The initiating event will be government declaring a phase 4 or 5 pandemic.<br>• If staff continue to work and are exposed to rest of population then consider monitoring health of families.<br>• After declaration of phase 4 pandemic, flights will gradually be reduced with no expected need to 'clear  the skies'. |
| **Phase 4: Short/Medium Term Actions (<48 hour)** |
| • Proactive decisions will be needed to gather and isolate key staff in major units.<br>• Training centre and all non-essential facilities will be closed with remote Internet/wireless communications to all homes in place.<br>• Other staff will be sent home but with plans to maintain currency and medical fitness for return to normal operations.<br>• Implement international agreements on over-flights during pandemic. |
| **Service Continuity** |
| **Phase 5 - Relocation** |
| • Military support may be moved to contingency facility if co-located with civil system to increase isolation and containment.<br>• Otherwise, staff movements will be avoided.<br>• Specific legal and administrative duties will be supported by staff 'on call' but work to be highly restricted.<br>• Safety staff will be available to assess risks of reduced operations. |
| **Phase 6 - Optimization** |
| • Corrective maintenance on all units.<br>• Continue contact with CFMU on optimisation of airspace.<br>• Electronic means of communication to be used rather than paper based exchanges with opportunities for contamination.<br>• Cash flow to be secured by finance department.<br>• Monitor isolation procedures and control disinfection of premised on regular basis. |
| **Recovery** |
| **Phase 7 - Longer-term response and Debrief** |
| • Once government has confirmed that pandemic is over, staff will gradually be brought in.<br>• Staged return reduces vulnerability to further waves in pandemic.<br>• Consultation with end-users and government on priorities for return to normal operation.<br>• Revise contingency plans to consider subsequent outbreaks as soon as possible. |

**Figure 8:** Case Study of Planning for Pandemics (Architecture Neutral).

*Internal Security Violations:* All of the previous approaches to contingency planning are also vulnerable to deliberate security violations by company employees. Although there is limited evidence about previous incidents across European and North American, other ANSPs have been blackmailed by former employees claiming to have introduced bugs and other deliberate flaws into ATM systems. Such threats are insidious and hard to rectify given the degree of 'insider knowledge' that such individuals may possess.

## Conclusions and Further Work

Over the last eighteen months, a project team from the European Organization for the Safety of Air Navigation has worked with a task force drawn from regulators and Air Navigation Service Providers (ANSPs) to draft guidelines for contingency planning. The intention is to help Air Traffic Management (ATM) organisations prepare for the potential loss of a major unit following scenarios that include terrorist actions, floods, fires and pandemics. As part of this work, a study was conducted to identify current and best practice in contingency planning. This paper has briefly introduced the different architectures that were identified. Some ANSPs have developed existing training facilities to act as fallback contingency centres. Other service providers have sought to reduce costs by ensuring that all of the regional control centres in a country are supported by a single national contingency facility etc. Our intention is to help service providers prepare resources for a wide range of threats to national safety-critical infrastructures. The closing sections have, therefore, considered a number of scenarios, including pandemics and software failures, that threaten to undermine all of the primary and contingency architectures mentioned in the previous paragraph. Further work is urgently required to develop appropriate risk assessment strategies to determine whether we can justify the high levels of investment that are required to address these scenarios. This is particularly important given that there are few agreed mechanisms for passing on the costs of contingency either to national governments, to airlines or to the passengers who may ultimately benefit from them.

## Biographies

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.

Gerald Amar, EUROCONTROL, Safety Security and Human Factors Division, Rue de la Fusée, 96, 1130 Brussels, Belgium, http://www.eurocontrol.int/esp, gerald.amar@eurocontrol.int

Gerald Amar is a EUROCONTROL safety expert, graduated from the French engineering school "Ecole nationale des Ponts et Chaussées". During the last fifteen years, he had been managing projects in different areas of Air Traffic Management. In 2007, he has managed the project to elaborate the "EUROCONTROL Guidelines for Contingency Planning of Air Navigation Services". These guidelines are available at http://www.eurocontrol.int/ses/public/standard_page/sk_sesis_guidelines.html

Tony Licu, EUROCONTROL, Safety Security and Human Factors Division, Rue de la Fusée, 96, 1130 Brussels, Belgium, http://www.eurocontrol.int/esp, antonio.licu@eurocontrol.int.

Tony has both ATC operational and engineering background (master degree in avionics). He worked in the past with both service provider organization and with safety regulator (ROMATSA the Romanian Service Provider and Romanian Civil Aviation Authority). He joined EUROCONTROL within Safety Regulation Unit in 1999 where he was responsible for several ESARRs (EUROCONTROL Safety Regulatory Requirements) namely with ESARR 2, 5 and 6 development, maintenance and/or promotion. He has managed within EUROCONTROL the Strategic Safety Action plan and since February 2006 is responsible for the European Safety Programme for ATM (ESP) implementation who oversee the Contingency Planning and Degraded modes of Operations work

Richard Lawrence, EUROCONTROL, Safety Security and Human Factors Division, Rue de la Fusée, 96, 1130 Brussels, Belgium, http://www.eurocontrol.int/esp, richard.lawrence@eurocontrol.int

Richard Lawrence is a former UK military air traffic controller and ATC safety manager who has extensive experience as a terminal and area controller working in the UK and abroad. Richard joined the EUROCONTROL in January 2006 as a Programme Coordinator for the European Safety Programme for ATM (ESP) and is the deputy project manager responsible for producing EUROCONTROL Guidelines for the Contingency Planning of Air Navigation Services.