ICAO International Civil Aviation Organization
North American, Central American and Caribbean Office

Project to Develop Guidance Material to Enhance the Resiliency of Air Navigation Services for the Caribbean Region

Aspects to Consider for
Improving the Resiliency of Air Navigation Systems

Prepared by:

Mr. Silvio J. Michelena Álvarez, Cuba
Mr. Pablo A. Luna Servellón, COCESNA

November 2023

Contents

INTRODUCTION

The resilience of ATS units depends on a group of technological and organizational measures.

Practical experience shows that there is a contradiction between the proposal of additional measures to the existing ones that increase the safety of operations and the cost that the implementation of such measures implies for the ANSPs, which will weigh on the expenses of the organization. This contradiction must always be analyzed by the directors of each ANSP and a balance point must be sought that allows guaranteeing the safety of air operations, with costs that are reasonably adequate.

Management commitment.

The preparation and implementation of contingency arrangements requires a very well-coordinated effort by the ATS service provider, which normally involves the entire Organization. For this, it is an essential condition to have the commitment of the ANSP management.

The declaration by the Organization's top executive regarding its commitment to allocating the necessary resources to preserve the safety and continuity of operations based on the systematic implementation of risk management procedures can be summarized in a contingency policy.

Analysis of the main issues that can cause a significant reduction in operational safety in an ATS unit.

The practice of the negative experiences recorded leads us to appreciate that the main issues in most of the events that cause reductions in safety in air traffic services, up to extreme contingency conditions (ATC0), can be grouped as follows:

I- Aspects related to the infrastructure of the ATS unit and services provided by third parties.

II- Aspects linked to the provision of CNS services by the ANSP

III- Other aspects

The aspects associated with the infrastructure of the ATS unit and the services received from third parties have generally been the main cause of effects on the ATS, as much or more than the aspects linked to the provision of CNS services. In this material we will analyze both aspects and the actions to improve the resilience of the system.

Many of the main measures to reduce technological impacts must be analyzed and implemented from the investment planning stage.

Taking actions to secure the infrastructure of an ATS unit, after it is operating, is possible, and often, unavoidable, but the execution of such actions in an ATS unit operating for 24 hours is a challenge.

ASPECTS RELATED TO THE INFRASTRUCTURE OF THE ATS UNIT AND SERVICES PROVIDED BY THIRD PARTIES

Failures in the energy systems.

Failures in the energy systems cause that, even if the most expensive and reliable equipment in the world is available, ATS services can be seriously affected if the most detailed measures have not been taken to ensure energy. Without reliable and uninterrupted energy there are no reliable services.

Elements to consider for the energy assurance of an ATS unit.

1.1- Evaluate whether your industrial energy provider can provide service from two nearby electrical substations or can transfer this energy to you by two independent means at an adequate cost.

1.2- Whatever the answer, it is very important that the main electrical node of your ATS unit has two generator sets, with automatic switching and with a power capacity, sized in such a way that only one of these two sets is enough to support the electrical load of the services, including the air conditioning systems for the technological premises and the controllers' room.

Having two generator sets and the required automatic control allows the continuity of the service in the event of failures of one of the two sets and during the periods in which one of the two sets is undergoing maintenance and its start-up must be blocked for safety measures. Whether it is a service contracted to a third party or the responsibility of an employee of the organization, that person will not be available instantly. In the contract with a third party or with an employee of your organization, you must consider the response times for such events.

1.3- The continuity of the electric power service from backup generator sets is particularly important during contingencies due to natural phenomena such as hurricanes, or other man-made phenomena, which can lead to very long periods of work with backup electric power during which strict monitoring of fuel stocks and periods of necessary maintenance and rotation of the backup sets must be maintained.

1.4- Current automated technological systems work with computing means that require guaranteed electric power, with 0 interruption time. A power failure for a few seconds can generate a complex restart of the systems that can take several minutes.

This reality requires that, in ATS units, the power of the automated and communications systems must be guaranteed with uninterruptible power backup systems (UPS).

Therefore, it is required that there are at least 2 UPSs with such capacity that only one of the two UPSs can manage the total load of the automated and communications systems of the ATS unit.

In UPSs, the UPS working time, i.e. the backup time, must also be sized. The action of the UPS does not consist of replacing the generator sets, but rather of keeping the equipment in service while the switching from the industrial network to the generator set is carried out, considering that the set could have some problem in the automatic start and require technical intervention for manual start. A practical criterion could be that the UPS have a backup capacity for a period of 30 minutes - 1 hour.

Another aspect to take into account is that the critical equipment of the main computing node (i.e. servers and network equipment, switches and routers) must have a double power supply, so that, in the event of a failure of some critical equipment source, the service is maintained. Critical equipment is understood as that equipment that causes a very significant affectation of the service due to a simple failure.

1.5- Another aspect is that the electrical distribution (wiring) between the sets and the UPS and between the UPS and the loads of the equipment to be backed up must be duplicated. The loads to be backed up should not be dependent on a single disconnector or electrical cable, which may turn off or present some type of occasional problem.

1.6- Finally, there is a last-ditch defense configuration that consists of the communications equipment, such as radios, telephones and VCSS, being powered by direct current (DC), that is, with batteries.

Advantages of DC electrical backup:

a) The accumulation of energy in batteries, only for the communications equipment, allows for a longer working time in the event of unforeseen interruptions related to AC power.

b) The batteries are installed close to the communications equipment, thus reducing the risk to the wiring.

c) In emergency situations, even if all surveillance has been lost, maintaining communications is vital to be able to manage the emergency and mitigate its consequences.

Failures in air conditioning systems

Practical experience has shown that there is a tendency to minimize the criticality of air conditioning systems in ATS units and it has been noted that this could be the second main cause of total service disruptions, leading to ATC0 disruptions.

Please, take in mind that air traffic control rooms are closed rooms, without windows and with relatively low ceiling struts, where there is a lot of equipment that gives off heat and also a number of people, with frequent rest times and with sufficient ventilation needs for their breathing. The option of fans can be annoying

for work, does not provide a comfortable temperature for controllers and causes undesirable noise in the room.

On the other hand, all current technological equipment, from UPS to communication nodes and computer nodes, dissipate a high thermal load, which forces them to work permanently with air conditioning systems.

Furthermore, all air conditioning systems require an exchange of fresh air with the outside, which may cause gases to be brought into the control room from a fire outside or from some other area of the building, a fire may be small and localized, but whose gases affect the health of the controllers.

On the other hand, a gas leak from some source or the impregnation of waterproofing chemicals or paints in the vicinity or on the roof of the building may cause an undesirable effect that causes risks to the ATS units.

2.1- No air conditioning system in ATS units should be simple. Even if it is a centralized air conditioning system, it must be composed of several machines and be at least duplicated for the controllers' premises and the critical technological equipment rooms.

2.2- The distribution of air conditioning and fresh air from outside and the return of hot air must be supported by ducts with the capacity to regulate (automatically or manually) the flows that allow the closing of this distribution channel of air conditioning or fresh air from outside, if necessary.

2.3- According to the consideration of costs, in the technological rooms of the critical equipment, an independent air conditioning equipment must be planned from the central air conditioning systems, if that is the climate solution of the building.

2.4- To the extent rational, the location of the technological equipment rooms close to the exterior walls of the building can be planned and ducts with air extractors can be installed to extract the hot air from these rooms, in case of total failure of the air conditioning equipment.

2.5- Finally, assess the risk that the air conditioning system cannot work due to power supply failures. In this assessment, study whether it is rational or feasible to increase the UPS capacity to provide backup power, for a time, to local air conditioning systems in technological rooms that could be affected by rapid increases in temperature due to lack of air conditioning.

Failures in the communications system infrastructure

This point refers to failures in the communications infrastructure that an external company is providing to the ANSP. It is useless to have the best and most expensive equipment in the world if we remain incommunicado with the outside world.

To do this, from the planning stage several measures can be foreseen:

1- Assess whether you can contract communications services from more than one local communications provider or if they can deliver the services with different technologies.

a) Bring the communications services to the ATS unit through underground cables, optical fiber or copper cables, or even better, in both ways.

b) Bring the communications services to the ATS unit through more than one underground communications system.

c) Bring the communications services through radio link or optical fiber, that is, through more than one communications support.

d) Bring the communications through analog links and digital links. Although all communications technologies are migrating to the digital environment, which is less expensive and more efficient, if the communications provider can maintain some services in an analog environment, this means that the ANSP will have its communications backed up.

e) Where possible, and the ATS units are located in the airport area, coordinate with the airport operator the different access points that the local communications provider can provide to keep its services vital to both organizations.

Each of the communications service variants must be assessed with your provider in terms of service quality agreements (SLA), costs and what these services represent in terms of vitality for your ATS unit.

2- Another good practice that is done in the States of our Region: VSAT communication eliminates the dependence of the ATS unit on local communications service providers for communications between ANSPs. To the extent rationally possible, maintaining some contingency communications services by VSAT is a good measure. Having VSAT communication as close to the ATS unit as possible increases the reliability of the service. Otherwise, there is a risk of rendering the measure useless.

3- Consider installing communication masts with antennas, if space is available in the vicinity of the ATS unit or on the roof, which allows you to have equipment for VHF radio communications or ADS-B receivers, which gives you an added advantage for the vitality of your unit. Generally, area control centers are close to the location of the country's main airport, so these means provide adequate coverage in the airspace near the country's main airport.

4- Consider locating these means in a nearby facility, with a direct line of visibility, and manage these communications with your own radio link if you do not have the space or geographic conditions to have the VHF or surveillance means of communication in the vicinity of the ATS unit.

5- Finally, having a common commercial telephone service, whether by landline, cell phone or satellite, and with a public Internet service can be a low-cost solution that solves a serious problem in the event of total communication failures in your ATS unit. This is a measure that can help you mitigate the effects of a serious contingency.

Other infrastructure failures to consider could be:

a) Structural damage to the building, including leaks or seepage that may affect operations in the ATS unit. Do not allow hydraulic pipes or leaks above the technological equipment or controller stations.

b) Health emergencies due to problems in the hydraulic or sanitation networks in a facility with a high concentration of people. A cessation of sanitary services to controllers can become a serious contingency.

c) Occasional activation of fire extinguishing systems can cause a serious problem for ATS services.

d) The review of aspects related to the physical security and protection of the facility are infrastructure issues that must be addressed.

All of these possible negative situations must be considered in the contingency plans, and must be taken into account, even from the investment stage of the facility, as possibilities to be faced at some point.

ASPECTS RELATED TO THE PROVISION OF ANSP CNS SERVICES

Redundancy in CNS equipment is vital for the correct provision of ATS services.

Redundant equipment significantly reduces the probability of affecting the services it provides. In general, all CNS equipment must be at least duplicated, that is, have a main equipment, a backup equipment and a monitoring and supervision device that allows switching, manually or automatically, if there are problems in its operation.

However, for the provision of ATS services it is not only about having redundant equipment, since we are talking about critical services, so redundant services must also be foreseen, based on the objective of minimizing the probability of contingencies occurring due to equipment failures.

So we are talking, for example, about having redundancies in:

- Multiple sites from which CNS services are provided. This prevents a failure at one site from causing a total failure, since the service can be provided from another site, in a complete or degraded manner, depending on the service in question.

- Multiple energy sources for each installation.

- Multiple communication channels, especially for Communications and Surveillance services, which must be available to controllers.

The CNS management indicators define that support management can be measured, both by services provided and by the facilities providing them.

There is a basic event indicator that represents the relationship between the number of events that affect a facility, the effect caused on the ATS service and the number of facilities to ensure the service.

This indicator provides an image of the level of security achieved by the CNS for ATS services.

Based on these concepts, and of course, on economic evaluation criteria (cost/benefit ratio), CNS systems are designed, always assuming that the equipment must be redundant and fail-safe.

Failures in the communication systems that contribute to the ATS

2.1- Failures in radio communication systems (ground-air communication).

VHF radio systems for controller-pilot communications are the basic support for ATC control. Without them, ATC is impossible.

Aspects to take into account to maintain the vitality of ground-air communications for ATC.

2.1.1- It must be foreseen that the radio stations for an area sector or TMA sector are located in more than one installation and have adequate over-coverage,

which allows the service to be maintained, even if there is a communication failure in one of the installations.

2.1.2- Reserve frequencies or secondary frequencies must be foreseen for an area sector or TMA sector to switch to working with them when the main working frequency is not available.

2.1.3- The selection of the site for the installation of VHF radio equipment must take into account the site's power facilities, including AC and DC backup power, the facilities available with the local communications provider, and the site's security against the possibility of vandalism, among others.

2.1.4- One aspect to take into account is that the radio equipment can work with both analog communications technologies and radios that support the new VoIP communication standards (ED-137). This makes it possible to contract more than one independent communications system (analog and digital) with the local communications provider.

2**.2- Failures in fixed oral communications systems (ground-to-ground communication, between ATS units).**

For the exercise of "seamless" ATC, an effective transfer of control between ATS units is required. This transfer of control will be more critical as the separation minimums are smaller in high-density traffic spaces.

2.2.1- An effective measure implemented among the States of the NAM/CAR Region has been the contracting of a VSAT communications system between the ANSPs of the Region, the well-known MEVA project. This has made communications reliable and independent of local communications providers. These VSATs should not be in facilities far from the ATS units because they lose their main advantage if they require communications between the VSAT and the ATS unit provided by a third party.

2.2.2- In the interest of having the greatest possible reliability for fixed communications, planning various technologies for them can be an effective and cost-effective measure. In this case, it is possible to negotiate with communications providers to establish services both by analog and by digital means (VoIP) without detriment to the requirements necessary for communications between ANSPs in terms of signaling forms and response times.

2.2.3- Furthermore, the organization of contingency oral communications between ATS units, supported by commercial telephone communications, allows controllers to have an economical way of maintaining the vitality of this service, if these communications are available at the controllers' stations.

2.3- Failures in the oral communication systems for controllers (VCCS).

For the exercise of ATC, oral communication is essential. All oral communications converge in a system, called VCCS, which is the one that orders and allows communication between the controller and any correspondent of the information, whether fixed or mobile. Therefore, the VCCS is an essential point to consider in the entire organization of communications and their contingencies.

Aspects to take into account when selecting a reliable VCCS:

2.3.1- The chosen VCCS must be free of simple failure points that compromise its work. In other words, it is not admissible that a simple failure takes down the whole. This requires a duplicate design of the central node equipment, from the network to the active equipment, including the computer equipment and the maintenance and configuration station. The double network must reach the work stations.

2.3.2- The chosen VCCS must be able to work both on frequencies and fixed communications, by traditional analogue and digital means. Analogue communication, currently more expensive and of lower quality, continues to be an important resource to maintain the vitality of communications because total failures are less likely to occur due to their very nature.

2.3.3- The communications network, external to the VCCS, must allow communication between the VCCS and the VHF radios that support the ED-137 protocol and between the VCCS and the VoIP telephone switching devices, usually based on the ASTERISK protocols, of the different ATS units.

2.3.4- The VHF radios, connected to the network through ED-137 digital protocols, must be configured to be connected immediately to other ATS units, which act as a contingency in the event of total failures in a given ATS unit. This contingency configuration must be systematically checked to ensure that it can be used when needed.

2.3.5- For VCCS operation:

2.3.5.1- Active network equipment or servers must have a dual power supply and be connected to a dual network.

2.3.5.2- The external network must be connected to the VCCS by more than one connection point.

2.3.5.3- The power supply must be supplied to the VCCS by more than one disconnect, from a UPS, and additionally, have the possibility of connecting the VCCS to a sufficiently sized DC backup source (batteries).

2.3.6- Finally, evaluate the costs associated with implementing an emergency communications system, independent of the main VCCS, that allows the controller, through a very quick action, to connect his headset or microphone to

a terminal device or connection box, which communicates with the radios directly, digitally, in the event of VCCS failures.

2.4- Failures in data network and aeronautical messaging systems (AFTN/AMHS).

The automation of processes linked to the CNS/ATM has led to a great dependence on automation and data networks. This means that the operation of the ATS unit depends heavily on this data network and aeronautical messaging.

2.4.1- The data network that connects your ATS unit to the rest of your organization must have sufficient protection measures, including network equipment, high availability servers and firewalls, intrusion detection and other security measures that allow you to reduce the risks associated with cybersecurity.

2.4.2- The ANSP data network must itself be a closed network, even if it has an extensive territorial scope. The points of contact of this closed network with its local communications providers for the extension of the WAN network or with networks of other ANSP organizations must be minimal and subject to permanent monitoring and supervision.

2.4.3- The necessary network protection measures may cause the creation of critical points in the information chain, which require the same measures to be taken with these critical points as those conceived for the central node equipment.

2.4.4- The costs and feasibility of having more than one point of contact between your local network (LAN) and the wide area network (WAN) that allows your ATS unit to be connected to the world outside your unit, within the ANSP network, must be evaluated with the local communications provider. Normally, a WAN network failure leaves your ATS unit without digital communications, without surveillance sources and without the exchange of aeronautical messages, at least.

2.4.5- The reliable way to interconnect their data networks must be evaluated with neighboring ANSPs. Keep in mind that a possible simple failure at an interconnection point deprives them of information exchange with the outside, as happens today when communication fails between any ANSP and the Atlanta AMHS Center for aeronautical messaging via the AMHS. The convenience and feasibility of achieving secondary communication for the AMHS, which does not depend exclusively on Atlanta, should be evaluated with neighboring ANSPs.

2.4.6- The feasibility of having a contingency system for aeronautical messaging via the Internet, such as the FAA has, consisting of AISR (Aeronautical

Information System Replacement), which allows access to aeronautical messaging information retained in Atlanta, in case of failures, which allows an effective mitigation measure, should be evaluated.

2.4.7- The AMHS Centers, with their corresponding AMHS/AFTN gateways, must be highly available and be as close as possible to the Area Control Centers and the regional link of the ANSP.

2.4.8- Introduce into your organization the best practices of the cybersecurity framework of the NIST (National Institute of Standards and Technology) of the United States that are being adopted by the international aeronautical community.

Failures in surveillance systems that feed into ATS units

Surveillance systems are also the basic support for ATC control. Without them, ATC is impossible when traffic density is high.

3.1- Aspects to take into account to maintain the vitality of surveillance systems.

3.1.1- It must be foreseen that there is more than one surveillance source for a given ATC sector and that they are located in more than one facility and have adequate over-coverage, which allows the service to be maintained, even if there is a failure in one of the facilities.

3.1.2- It must be foreseen that the main air flows of an ATC sector are monitored by more than one source and that the cone of silence of a radar is well covered by the work of another surveillance source.

3.1.3- By their very nature, ADS-B and MLAT surveillance sources require reliable digital links with adequate performance. In economic terms, ADS-B and MLAT surveillance sources are lower cost investments than radar, but they have other characteristics that allow us to conclude that the best strategy is to combine the different sources.

3.1.4- The selection of appropriate locations for the installation of surveillance systems must take into account the power facilities of the site, including AC and DC backup power, communications facilities available with the local communications provider and site security against the possibility of vandalism, among others.

3.1.5- One aspect to take into account for communication with radars is that the transmission of surveillance information can be carried out indistinctly with analogue (via modems) or digital communications technologies. This makes it possible to contract more than one independent communications system (analogue and digital) with the local communications provider.

3.1.6- The feasibility of having more than one link between the surveillance source and the ATS unit must be evaluated with your communications service provider.

3.1.7- ADS-B stations are the most economical surveillance sources and generally provide quality data, but they are dependent surveillance sources and in a surveillance system they must be combined with independent surveillance sources such as radars and MLAT systems.

3.1.8- In complex surveillance sources (radars, MLAT systems, ADS-B signal concentrators) the equipment must be duplicated, with a double network and backup power supply systems.

3.1.9- The diversity of different surveillance sources and in different facilities allows surveillance to be maintained, even during the occurrence of adverse meteorological phenomena that force the disconnection of some of them during these meteorological events.

3.2- Aspects to take into account to maintain the vitality of automated air traffic control systems.

Automated air traffic control systems are the technological link available to ATC to allow the human-machine interface (HMI) and a failure of these systems causes a significant reduction in the security of the services, which can lead to ATC0.

3.2.1- Automated air traffic control systems must be free of single points of failure that compromise their work. This requires a high availability design of the central servers, the network and the active equipment. The double network must reach each workstation. Both the servers and the network asset equipment must have duplicate power sources.

3.2.2- The interface server (SIF) with the surveillance sources must be able to connect to the surveillance sources through both digital links and low-speed analog links.

3.2.3- The main systems of an air traffic control system are the surveillance data processors (SDPS) and the flight plan data processors (FDPS). The system as a whole must provide for the fact that a failure of the SDPS allows the continuity of the work of the FDPS and vice versa.

3.2.4- The system design must provide for the fact that, in the event of a failure of the SDPS servers, the work positions have direct access to the surveillance sources, selected by the sector controller, in order to maintain, at the time of the contingency, situational awareness of what was happening at the time of the event.

3.2.5- The system design must provide that, in the event of a failure of the SDPS servers, at the discretion of the operational supervisor, the movement of the stopped tracks is optionally activated, by generating the movement of synthetic

tracks, taking into account the latest information stored in the flight plan servers to maintain, at the time of the contingency, situational awareness of what was happening at the time of the event.

3.2.6- When the density of air traffic justifies it, and through a prior evaluation of the costs, each working sector must be composed of two control positions with the same characteristics, to meet the demands of the sector. This design allows the simple failure of any position in a work sector to be excluded from contingencies.

3.2.7- The double positions of each work sector must have data network wiring and an independent power supply, if possible, from independent disconnectors.

3.2.8- One of the main causes of disruptions in automated air traffic control systems is software updates, which respond to new service requirements or to improvements already solved in previous versions. These software updates are generally complex and cannot be fully tested in the software manufacturers' environments. Hence, the importance of having an automated test system, which receives the same surveillance data and flight plans as the production system and where exercises can be designed to check the adaptation of the software to meet the requirements, whether they are new requirements or those that existed before the software update.

3.2.9- The best time must be chosen for system software updates, even if said updates have been sufficiently tested in the test systems. Updates must always be made at times of less potential disruptions and on dates not close to weekends, holidays or commemorative days, with the required specialized IT personnel available and having secure procedures for restoring the previous version to the current update. Always be very cautious, systems are becoming more and more complex.

Failures in radio navigation aid systems

Radio navigation aid systems are the branch of air navigation where global systems have been most widely used. Of all the actions arising from the implementation of the CNS/ATM concepts by ICAO, global navigation systems are the most technologically mature, and the concepts of GNSS, PBN, RNAV and RNP were developed.

However, this does not mean that we forget that we must have more than one option to allow safe air navigation, depending on the requirements of a given airspace.

4.1- To our knowledge, no State or organization has so far completely dispensed with ground-based radio aids, although the trend is towards their gradual elimination. NDBs practically no longer exist and VORs are being deinstalled, although some remain, which serve as an option for navigation in the event of occasional degradation of the GNSS signal.

4.2- ILS and DMEs, whether in the composition of VORs, ILS or for multi-DME navigation, remain a valid option and, in the case of ILS, they still allow for lowering landing minima to a point where RNP procedures have not yet reached.

4.3- As a summary of this situation, the contingency foreseen for air navigation radio aid systems consists of:

a) Developing air routes and RNP or RNAV departure and arrival procedures to take advantage of the benefits offered by GNSS.

b) Maintaining, after an assessment of economic feasibility, a group of ground-based radio aids, which allow safely supporting air traffic in areas with the highest flow density in the event of occasional failures of the GNSS signal.

c) Continuing with the assessment of the economic feasibility for the deployment of augmentation systems that allow compliance with integration requirements, and above all, integrity, of the GNSS signal.

OTHER ASPECTS THAT CAN CAUSE CONTINGENCIES IN ATS UNITS

Finally, we would not like to conclude without mentioning other aspects to which maximum attention must be paid, in order to prevent events that cause contingencies in ATS units.

a) Aspects of the food and health of the controllers

It must be taken into account that ATS services always require controllers. Therefore, the health of the controllers must be the object of permanent attention, which must be stricter in view of the possibility of contagious diseases. The COVID19 epidemic and its consequences on the provision of services in many ATS units are still close in time.

A possible source of affectation of the health of the controllers is related to water and food, which can cause digestive problems, with serious effects on the service they provide. In this regard, the most basic measures are the most effective, but they must always be taken into account.

b) Natural disasters (hurricanes, earthquakes, floods)

The possibility of natural disasters occurring must always be considered in contingency plans. These disasters can affect ATS services for long periods of time and in large areas of territory, and the impact on ATS services can have negative consequences for dealing with the consequences of disasters.

Natural disaster recovery plans must be part of contingency plans and also provide for the necessary coordination with neighboring ATS units to maintain services on contingency routes.

c) Human-caused events (social unrest, war, sabotage)

Finally, although less frequent, the occurrence of human-caused events that cause impacts on the provision of ATS services must also be foreseen in contingency plans, even though their occurrence and consequences are difficult to predict.

CONTINGENCY STRATEGIES FROM ENGINEERING SYSTEMS PERSPECTIVE

GENERAL

It is important to highlight the critical role played by technical/engineering personnel in the event of a contingency.

For example, in the 'Co-located' and 'Multi-use' sector strategies, ATS system 'reconfiguration' is briefly mentioned as a key systems engineering factor during the Short/Medium Term Actions and/or Relocation phases. Indeed, in some cases ANSPs' systems engineering approaches are likely to have a strong influence on the selection of the ANSPs' overall contingency strategy.

This section addresses the essential contribution of air traffic services engineering personnel during contingency and describes how various engineering approaches can affect contingency planning.

DIFFERENT ENGINEERING APPROACHES TO CONTINGENCIES

The main engineering support approaches identified are:

- In-house engineering.

- Contractors and Subcontractors.

- Use of 'Commercial Off the Shell' COTS equipment.

- International Technical Letters of Agreement (LOA).

- Cooperation on Cross-Border Infrastructure

These approaches are NOT mutually exclusive and any ANSP is likely to have a mix of each. Some ANSPs rely heavily on outsourcing key infrastructure elements

including hardware and software applications. Others retain a significant software development function such that both develop and maintain the majority of their applications:

The learned lessons identify the potential risks of each engineering approach and how these could impact the ANSPs' ability to execute their chosen contingency strategy(ies).

The risks and actions to mitigate them are listed below.

'IN-HOUSE' ENGINEERING

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

KEY FEATURES

- Specific solutions are tailored to local needs.

- This limits the opportunities for 'commercial off-the-shelf' (COTS) solutions.

- ANSPs retain considerable internal resources for the development and maintenance of their ATS system infrastructures.

- Internal communication is suitable between systems engineers and operational staff because both are employed by the same organisation.

POTENTIAL CONTINGENCY RISKS

- Systems engineering teams rely on a relatively small number of people with the most experience and primary knowledge of technical systems.

- Limited number (e.g. one or two) of people who have the necessary skills to support the transfer of systems infrastructure to a contingency site.

- Potential vulnerability, few technical backup staff, for some contingencies related to staff availability (e.g. disease, terrorist attacks and pandemics).

- Key engineering staff may be required to identify the causes of the contingency and also to activate an alternative facility leading to staff shortages.

MITIGATION ACTIONS

During the planning phase:

- Identify potential vulnerabilities and skills shortages in systems.

- Define appropriate solutions to address staff shortages (including technical/engineering staff) in case of staff-related contingency scenarios (e.g. disease, pandemics, strikes, major security breaches).

- Also, carefully address the impact on “engineering support” capability from the absence of core technical experts in the ANSP upon leaving the company or retiring.

CONTRACTORS AND SUBCONTRACTORS

The increasing complexity of many ATS systems often prevents ANSPs from maintaining specialized expertise in the development and maintenance of all the applications on which they depend. Consequently, ANSPs may subcontract specialists to maintain their systems. This approach creates specific demands for contingency support.

KEY FEATURES

- Complex CNS or ATS systems or subsystems.

- ANSPs subcontract development and maintenance expertise to external contractors.

- Contractors may be required to support contingency operations (emergency, degraded modes of operation, and continuity of service).

- Contractual agreements are necessary to explicitly state the scope of support that an ANSP can expect from a contractor under contingency conditions.

- Liaison with contractors and subcontractors is necessary during the contingency planning phase.

POTENTIAL CONTINGENCY RISKS

- Contractor support during contingency operations is outside the ANSP's administrative control;

- Contractor engineering support (effectiveness, schedule, etc.) may be insufficient to meet contingency requirements.

- Contractors' dependence on subcontractors may lead to increased complexity and risk.

- It is extremely difficult to foresee the range of constraints that could impact the ability of external agencies to deal with contingency situations, for example during pandemics or major security failures.

- Contractors may not be familiar with all aspects of an ANSP's safety management system and may have very different views regarding safety culture both before and during the contingency. This problem can be exacerbated when prime contractors employ a variety of additional subcontractors who have only an indirect relationship with the ANSP.

- Communication problems can increase as ANSP management has to deal with contingencies and also arrange for the necessary support from external contractors.

- In some States there may be a monopoly on the provision of infrastructure, especially in communications. These companies may not be willing to meet the service levels expected by ANSPs under contingency conditions. These monopolies may also lack the technical resources to provide the levels of reliability and support anticipated by ANSPs.

MITIGATION ACTIONS

- ANSPs should ensure that external agencies meet the requirements created by particular contingencies.

- External engineering support should be formalized through contractual instruments (e.g. warranties and service level agreements). These documents should consider the guaranteed number of personnel and time that an ANSP may require from a contractor under contingency.

- Such agreements should establish the quality and level of engineering support to be provided by external contractors in the event of particular contingencies.

- The involvement of subcontractors in supporting contractors should be clarified. Requirements should be cascaded down to subcontractors.

- Conduct joint training and exercises with contractors and subcontractors, especially when contracted personnel must be transferred from other projects and sites to help ANSPs respond to a contingency and anticipate communication problems that might otherwise delay an effective response to any future incident.

- Contingency planning experience has shown that the contractor/subcontractor relationship can create many one-off issues that are only seen during complex exercises.

- Clarify decision-making lines from ANSPs down to the subcontractor level, for example, subcontractors may find it difficult to identify individual managers with the authority to make critical engineering decisions immediately following a major system failure.

- Carefully address scenarios that impact the availability of external staff, such as major security failures or pandemics.

- Carefully address the availability of external engineering support in scenarios that consider moving ATCO staff to another site.

- Implement monitoring systems, for example on local area networks, to help diagnose the source of complex system failures that may arise from complex

interactions between internal applications and systems maintained by subcontractors.

- Measures can be taken to ensure that outsourced personnel are integrated into the ANSP's safety management systems prior to a contingency.

- In some places, where ANSPs are required to work with monopoly suppliers, in order to achieve the highest possible levels of assurance for contingency provisions before an adverse event occurs, validation measures should be in place to ensure that, for example, national telecommunications companies can meet ANSP requirements and understand the critical nature of the services they provide to ATS operators.

'COMMERCIAL OFF-THE-STOP' (COTS) APPROACHES

More and more CNS/ATM systems include COTS elements. This trend is likely to increase in the future with current developments in interoperability and product development by ATS system manufacturers. This will continue in the future under pressure for standardisation and interoperability.

KEY FEATURES

- Several elements of ATS systems and CNS infrastructure are COTS.

- Use of COTS limits ANSP engineering staff's direct access to equipment (hardware and/or software):

- There may be only limited opportunities for ANSP engineers to directly access the underlying code for technical and business reasons, for example real-time operating systems.

- Problems may arise from complex interactions between COTS components and other custom elements of the ATS infrastructure. It may be difficult to diagnose intermittent faults arising from COTS systems if ANSPs cannot look inside those components to identify the subsystems that are failing.

POTENTIAL CONTINGENCY RISKS

- ANSP support engineering staff may not be able to perform required actions on hardware/software during contingency operations, for example engineering staff do not have direct access to hardware or software to perform repairs or debugging.

- These problems may be exacerbated if COTS components have been installed by subcontractors who do not have direct access to the engineering details of the systems they have provided.

- During a crisis/contingency, there is often a pressing need to contact suppliers to intervene on site and/or hire experienced personnel at short notice to supplement internal engineering resources.

- This can create considerable problems when, for example, some knowledge of ATS operations may be required in addition to skills in operating COTS applications.

- Original suppliers may not be aware that their application is being used in a particular configuration within an ANSP's infrastructure and may therefore only be able to offer limited support.

MITIGATION ACTIONS

During the planning phase:

- Maintain an ongoing agreement between ANSP and engineering support provider

- Define precisely with the COTS provider (or other third party):

• What level and quality of support provided: type of support, reaction times, replacement times, repair time

• What availability (e.g. H24, Weekend)?

• What stock of backup supplies?

- Participate in suppliers' reporting and updating schemes to ensure the ANSP can learn from any previously reported incidents.

- Implement monitoring systems, for example on local area networks, to help diagnose the source of complex system failures that may come from COTS applications.

TECHNICAL LETTERS OF AGREEMENT

Several States operate the same basic technical systems, which have been tailored to their particular operational needs. This may be particularly appropriate.

KEY FEATURES

- International letters of agreement extend beyond immediate operational requirements to provide broader systems support.

- Several ANSPs have begun to develop agreements for the joint management of common infrastructures. These agreements provide a model for the exchange of technical support in the event of a contingency.

- Systems engineers from one ANSP may be sent to assist those from an affected unit in another country.

POTENTIAL CONTINGENCY RISKS

- Similar to concerns about ATCO licensing and training, the same concerns arise about the legal status, competence and certification of individual support engineers working on another country's infrastructure.

- It may also not be possible for other ANSPs to provide people with the appropriate level of technical expertise in time to help address a contingency in a neighbouring State.

- There are few examples of engineering personnel being deployed to assist an ANSP from another State, in time to respond effectively to a contingency. This approach therefore remains untested, even if the situation may change with the increasing use of common infrastructure components.

- It is important not to underestimate the communication problems that may arise between employees of different ANSPs. These extend beyond procedural differences affecting technical operations and include different attitudes towards many aspects of Security Management.

- There is a risk that sharing systems personnel under contingency may introduce more risks than it resolves, as such individuals may not fully understand the detailed engineering of another ANSP's infrastructure.

MITIGATION ACTIONS

During the planning phase:

- Address, as necessary, the legal status, competence, and certification of support engineers provided by other countries.

- Technical and engineering exchanges should be conducted before a contingency occurs so that personnel become familiar with the SMS environment and procedures in a neighboring State well before a contingency occurs.

- Define with neighboring ANSPs realistic requirements in terms of support staff availability.

- Do not overestimate the level of expertise to be provided.

- Do not underestimate the familiarization needed with their operating systems and environment.

- Carefully address logistical aspects (travel, arrival, insurance, lodging, facility management, etc.).

After contingency execution, within the post-event analysis:

- Brief "foreign" engineering support staff before they return home.

- Avoid bad publicity by ensuring that deficiencies are not ignored.

- Review contingency arrangements accordingly. Many of the mitigations for subcontractors also apply here given that employees of another ANSP will face the same communication problems that complicate the role of external agencies under contingency conditions.

CROSS-BORDER INFRASTRUCTURE COOPERATION

A number of States rely on their neighbours for critical elements of their infrastructure provision; for example, geography may dictate that ANSPs have to use radars and communications systems from other States to maintain service levels across the Region in sea areas where they would otherwise be unable to provide CNS functions.

KEY FEATURES

- Geographical and technical constraints of some States may result in some ANSPs being dependent on their neighbours for their engineering support systems: for example, if a service provider has no land mass available on the periphery of an offshore FIR, it may request data from a neighbour's radar site covering elements of its airspace.

POTENTIAL CONTINGENCY RISKS

- This creates two issues for contingencies: how to ensure that the loss of these services in neighbouring ANSPs does not trigger a contingency and also how to ensure that such services can be maintained under contingency when technical staff from other States may be needed to work on other CNS requirements of the neighbouring State.

- Changes to the infrastructure of the State hosting remote services may disrupt the flow of CNS data between neighbouring States and this may trigger a contingency.

- Routine maintenance and upgrades to remote infrastructure are not under the control of the ANSP sharing these services. This may exacerbate existing problems; for example, requiring ANSPs to use procedural control techniques.

MITIGATION ACTIONS

During the design and implementation of contingency provisions, ANSPs can increase the resilience of CNS connections with neighbouring States, for

example, by using satellite links that are less vulnerable to breaks that may affect marine data cables or by creating multiple cables to ensure redundancy in transmissions between States. Personnel may need to be trained on appropriate procedures to be used when remote elements of the infrastructure are lost.

Systems engineering teams should be provided with effective communications support so that they can quickly contact their colleagues in the neighbouring ANSP in the event of interruptions to remote CNS data flows.

A LIFE CYCLE APPROACH TO CONTINGENCY SYSTEMS ENGINEERING.

The provision of contingency systems engineering must change over the life cycle of ATS applications.

As illustrated above:

- Many major systems are initially outsourced to specialized suppliers.

- As the system progresses from the initial installation phase, ANSP systems engineering teams must gradually become familiar with the underlying architectures and technologies.

- Suppliers and systems integrators act as external contractors, although they may spend long periods working on-site with the ANSP.

- Over time, internal systems engineering teams are often trained to take responsibility for maintaining infrastructure systems from the initial supplier.

- ANSP systems engineering teams also gradually assume greater control and independence in coordinating technical response to any contingency. Or it may happen that the original supplier is given responsibility for maintaining the system - when this happens 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 then arise in some ANSPs where there may not be the same "defenses in depth" that are provided in larger ANSPs. Similarly, there may not be the same range of in-house technical support to "cope" when the vendors hand over the equipment if subsequent problems arise.

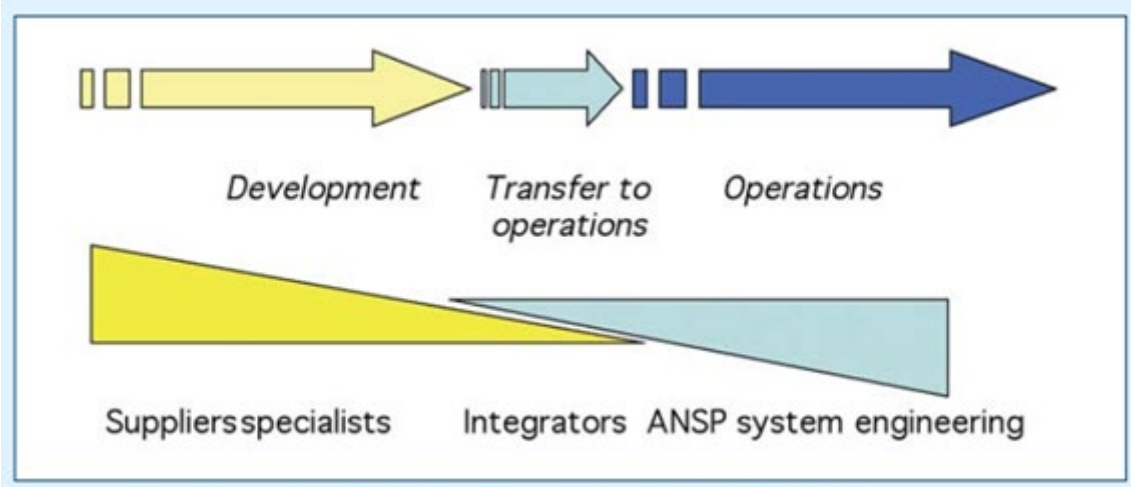
As changes are introduced to the initial release of the system:

- The external vendor may lose the necessary contact with the system as it evolves. This may reduce their ability to provide immediate assistance during any subsequent contingencies.

- Even if a vendor continues to provide on-site support, the initial development teams may be replaced by technical staff who do not understand the detailed underlying engineering of an application that may be needed under a potential contingency.

- Detailed contingency plans should therefore consider both the needs of internal and external staff for a range of core infrastructures as the identity and nature of these systems will change over time.

- The impact of changes to the support of engineered systems should be considered in contingency planning within the broader forms of risk assessment carried out before new applications are handed over to an ANSP.



Suppliers and ANSP Engineering staff vis a vis ATM Life Cycle

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 facility will fail completely at the same time as considerable efforts have been made to eliminate single points of failure. However, there are differences in the different partial failure modes that complicate the response to contingencies:

- Intermittent failures. A failure may appear, for example, within CNS applications, for a short period of time and then 'resolve' itself before engineering staff can identify the cause. This can occur when periodic failures affect hardware components. However, unless the cause is identified, there is a considerable risk that a worse contingency may occur if the failure returns. The ANSP should work with contractors to implement sufficient monitoring resources to diagnose the cause of intermittent failures.

- Partial Loss of Subsystems. It can be difficult to identify the precise causes of failure when only a small number of systems appear to be affected. Failures can arise from the interaction of applications provided by several different engineering groups within an ANSP or from different vendors. This creates considerable problems in identifying who is required to respond to a contingency situation.

3.2 CONCLUSION

Finally, it is important to stress that only a brief overview of potential system failures and how to improve system resilience has been provided here.

Each ANSP must ensure that its systems engineering strategy is fully compatible and integrated with its overall approach to contingencies.