ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

A UN SPECIALIZED AGENCY

Identification of Contingency Scenarios and Impact Assessment

Module 2

Silvio J. Michelena Álvarez

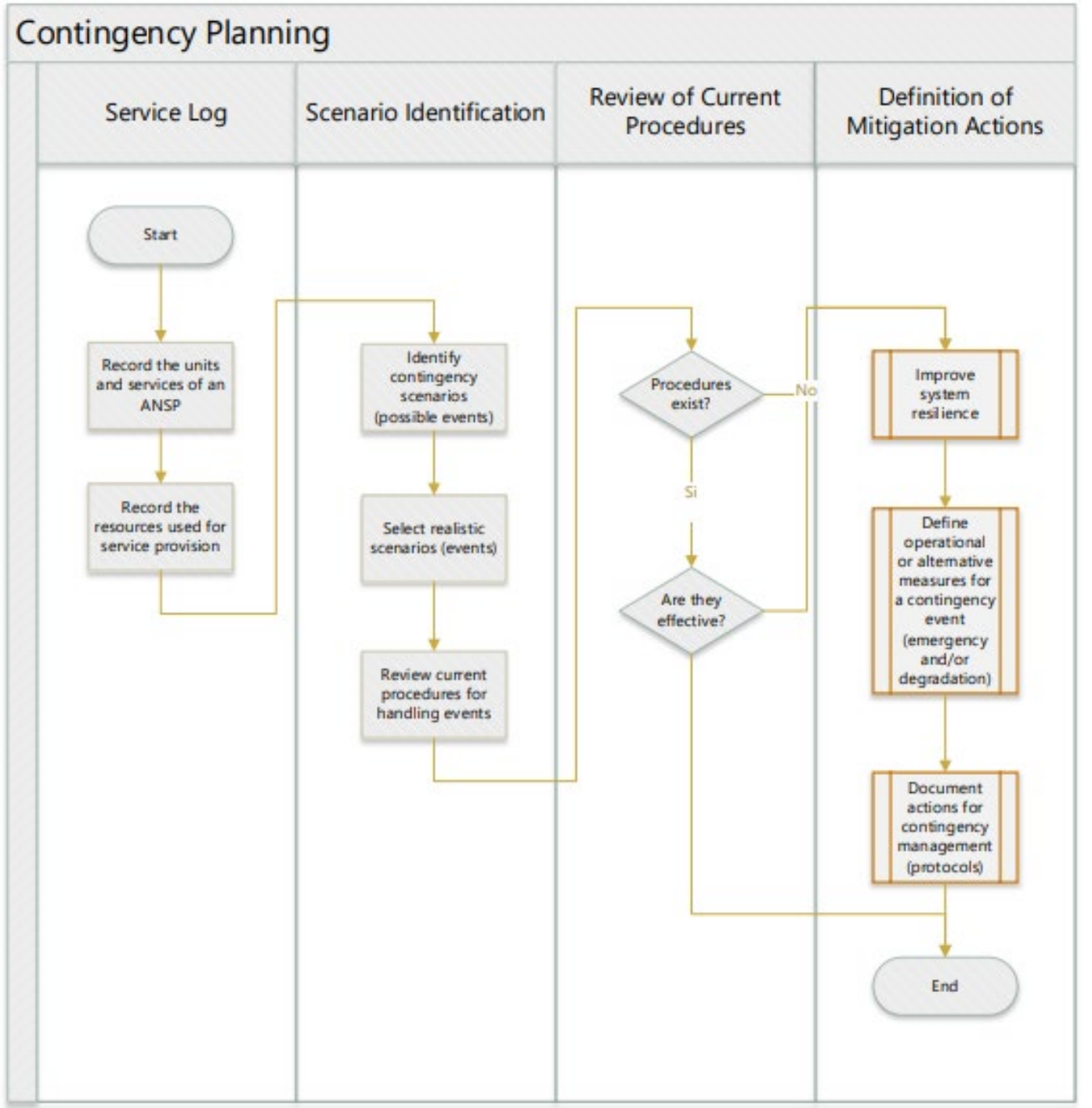
Pablo A. Luna Servellón

ICAO

Module Objectives

- Develop capabilities to identify realistic scenarios that affect normal operations and consider appropriate contingency measures for each event.

- Provide tools and promote discussion and debate on situations, reaching consensus on defining contingency actions that allow air operations to continue to meet the safety requirements defined for each ANSP.


Contingency Planning
Service Log
Scenario Identification
Review of Current Procedures
Definition of Mitigation Actions
Start
Record the units and services of an ANSP
Record the resources used for service provision
Identify contingency scenarios (possible events)
Select realistic scenarios (events)
Review current procedures for handling events
Procedures exist?
No
Si
Are they effective?
Improve system resilience
Define operational or alternative measures for a contingency event (emergency and/or degradation)
Document actions for contingency management (protocols)
End

Module Content

01 Record the units and services of an ANSP

02 Record the resources used for service provision

03 Events that disrupt normal operations

04 Process for determining realistic events

05 Risk assessment to be included in the contingency plan

06 Tables for identifying realistic contingency scenarios

Record the units and services of an ANSP

The first step in contingency planning is to identify, as broadly as possible, the portfolio of services/functions that an ANSP provides to all its customers. For example, at the "service" level, an ANSP may provide ATS (en-route, approach, and tower), which, at the "functional" level, will involve the provision of VCCS, surveillance, FDPS, etc.

Similarly, ANSPs could list all service and/or product providers whose failure may affect their provision of air navigation services/functions:

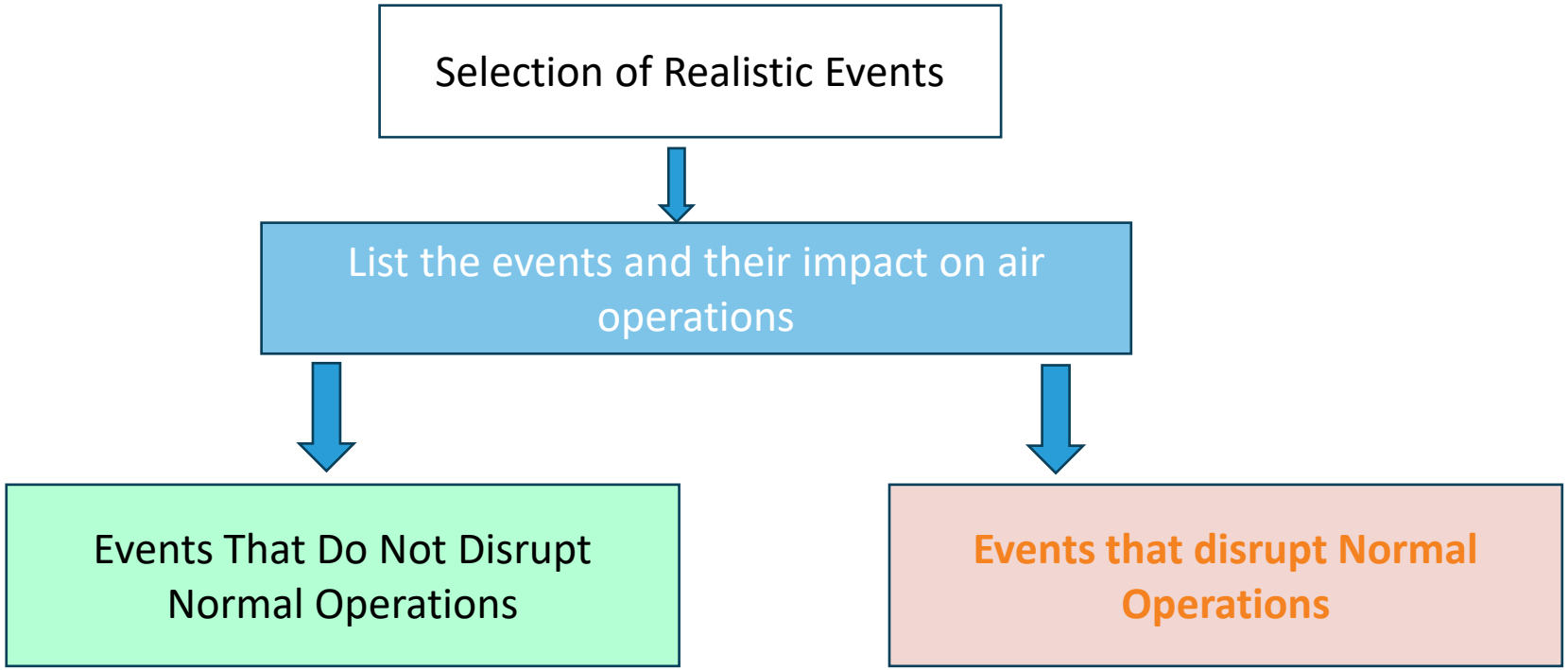
1- List the ANS units (e.g., TWR, APP, ACC, describing the working sectors, etc.)

2- For each unit, list the services/functions (e.g., Communications, Navigation, Surveillance, Data Processing System) provided for each unit, including external providers.

For example:

- Air Navigation Services and Unit Support Services (e.g., AIS, MET, CNS);
- Services from other non-ANS providers (e.g., IT, energy assurance, etc.)

Selection of "Realistic Events"



Events That Do Not Disrupt Normal Operations

These are events whose conclusions from the security assessment are incorporated into the operations manuals, operational and technical personnel are notified, and measures to be taken in the event of certain failures are implemented.

Some of these failures do not affect normal operations due to their very nature and because the ATM system/service architecture is tolerant to these failures. They are disclosed as part of training or after an event through informational notices that share lessons learned.

Examples

- Loss of a display in a sector (when the sector consists of more than one display and has at least two air traffic controllers, both with surveillance screens).

- Loss of a radar site, provided that the number of remaining radars available is at least equal to the minimum number of radars required to operate a sector normally.

- Maintenance intervention on equipment whose level of redundancy allows for maintaining normal operations.

Events that disrupt Normal Operations

These events cause or may cause the loss or interruption of the air navigation service or function provided.

Processes and criteria for identifying events that disrupt normal operations.

- Event and incident database (if applicable).
- Comparative evaluation (exchange with other air navigation service providers).
- Systematic analysis.

Filtering process to determine realistic events

Events should be considered "realistic" when:

- regulation requires mitigation of their consequences,
- they have already occurred before, e.g., their occurrence is recorded in databases,
- they have been experienced by another ANSP in a similar operating environment,
- they are equivalent to another "realistic" event or linked through a chain of events.

Events should be excluded when there is a reason why they cannot be considered "realistic."

An event is not realistic:

- when the event is unlikely to occur, and for which there are no direct or indirect mitigation measures, therefore, the risk is considered negligible and is accepted, e.g., a meteorite striking the ATC or an earthquake exceeding a given magnitude in an area with no records of such activity.

- when it is associated with or equivalent to another unrealistic event.

The decision to exclude realistic events must be documented.

The result of this step is to obtain, for each ATS unit, a consolidated list of events that could realistically lead to a loss or interruption of services.

Process and criteria for identifying events that disrupt "normal operations"

Events can be collected through brainstorming by the ANSP's various technical and operational departments (including ATS and SMS).

This brainstorming can be supported by lists, logs, or event histories:

- Event/incident database (if one exists);
- Benchmarking (exchange with other ANSPs);
- Systematic analysis.

Realistic events could include:

Potentially frequent situations (e.g., partial loss of radar coverage) where disruptions would partially affect ANSPs for short periods of time (ranging from a few hours to a few days).

Rare but high-impact situations (e.g., major software errors, floods, earthquakes, terrorist attacks, pandemics, in which entire ATS units could be completely out of service for extended periods of time).

Document 9859, "Safety Management Manual," provides sufficient guidance to determine which realistic events we should consider in a contingency plan.

Events can be of different categories:

- ATM-related events
- Building infrastructure/air navigation service provider events (fire, power supply, ICT service provision)
- Environmental events (floods, earthquakes, chemical contamination)
- Security-related events (terrorism, sabotage, hacking)
- Aviation threats (hijackings, plane crashes)

Some CNS/ATM related events

- Loss of the SDPS server or communications with surveillance sources for more than X seconds
- Total loss of runway correlation for more than X seconds
- Loss of SSR code assignment management
- Loss of information display on system clients
- Loss of STCA, MSAW, or other functions
- Loss of the FDPS flight plan management server or aeronautical messaging communications for more than X minutes

Some CNS/ATM related events

- Loss of air-ground communications for more than X seconds
- Total or partial loss of ground-ground communications for more than X minutes
- Loss of AIDC function in one or more work sectors for more than X minutes
- Loss of the flow management unit's working capacity for more than X minutes
- Loss of technical or operational supervision for more than X minutes

Aspects related to infrastructure or services provided by third parties have generally been the fundamental cause of the impacts on the ATS.

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

Taking action to secure the infrastructure of an operational ATS unit is possible, and often unavoidable, but implementing such actions requires careful planning and execution, as well as risks that must be managed during the implementation of such measures.

Some events related to third-party infrastructure or services

- Severe damage to the building structure due to various causes
- Severe damage to the building structure due to natural events
- Total loss of power supplied to the building
- Loss of communications services provided by third parties
- Loss of drinking water or sanitation services to the building

Likelihood	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

Table 1. Safety risk probability table

Severity	Meaning	Value
Catastrophic	• Aircraft / equipment destroyed • Multiple deaths	A
Hazardous	• A large reduction in safety margins, physical distress or a workload such that operational personnel cannot be relied upon to perform their tasks accurately or completely • Serious injury • Major equipment damage	B
Major	• A significant reduction in safety margins, a reduction in the ability of operational personnel to cope with adverse operating conditions as a result of an increase in workload or as a result of conditions impairing their efficiency • Serious incident • Injury to persons	C
Minor	• Nuisance • Operating limitations • Use of emergency procedures • Minor incident	D
Negligible	• Few consequences	E

Table 2. Example safety risk severity table

Safety Risk Probability		Severity: Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent	5	5A	5B	5C	5D	5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3	3A	3B	3C	3D	3E
Improbable	2	2A	2B	2C	2D	2E
Extremely improbable	1	1A	1B	1C	1D	1E

Table 3. Example safety risk matrix

Safety Risk Index Range	Safety Risk Description	Recommended Action
5A, 5B, 5C, AA, AB, 3A	INTOLERABLE	Take immediate action to mitigate the risk or stop the activity. Perform priority safety risk mitigation to ensure additional or enhanced preventative controls are in place to bring down the safety risk index to tolerable.
5D, 5E, 4C, 4D, 4E. 3B, 3C, 3D, 2A, 2B, 2C, 1A	TOLERABLE	Can be tolerated based on the safety risk mitigation. It may require management decision to accept the risk.
3E, 2D, 2E, 1B, 1C, 1D, 1E	ACCEPTABLE	Acceptable as is. No further safety risk mitigation required.

Table 4. Example of safety risk tolerability

Realistic events that generate intolerable risks must all be included in the contingency plan

Realistic events that generate tolerable risks should be evaluated, and a consensus should be reached to determine whether or not to include them in the contingency plan.

THERE ARE NO UNIVERSAL FORMULAS FOR CONTINGENCY PLANNING FOR EACH INDIVIDUAL ANSP.

It requires teamwork and a great deal of analysis.

	Services required for ATS units (for each ACC sector)	Service facilities	Probability Assessment	Impact assessment
1	Communication services			
1.1	Air - Ground Communications			
1.1.1	Main frequency radio, each sector			
1.1.2	Secondary frequency radio, each sector			
1.1.3	Control Working Position of VCSS, each sector, for A-G links			
1.2	Ground - Ground Communications			
1.2.1	Ground- Ground voice line with sector A			
	Ground- Ground voice line with sector A			
	Ground- Ground voice line with sector A			
	Ground- Ground voice line with sector A			
	Ground- Ground voice line with sector A			
1.2.2	Control Working Position of VCSS, each sector, for G-G links			
2	Surveillance			
2.1	Information from surveillance sources			
2.2	SDPS (Surveillance Data Processing System)			
2.3	Surveillance Control Working Position, each sector			
3	Flight plan processing			
3.1	Aeronautical Messaging (AFTN or AMHS)			
3.2	FDPS (Flight Data Processing System)			
3.3	Flight Data Control Working Position, each sector			

	Services required for ATS units (for each ACC sector)	Service facilities	Probability Assessment	Impact assessment
4				
4.1	Information from weather sensors (if any)			
4.2	Access to processed meteorological information (METAR, TAF, SIGMET, satellite images, radar images)			
4.3	Access to processed AIS information (NOTAM, AIP, AIC, SUP)			
4.4	Display for AIS/MET information, each sector			
5	Navigation			
5.1	Navigation based on ground-based aids, each ATS sector (if any)			
5.1.1	VOR/DME			
5.1.2	ILS			
5.2	GNSS-based navigation (RNAV or RNP), each ATS sector			

	Services required for ATS units (for each ACC sector)	Service facilities	Probability Assessment	Impact assessment
1	Energy supplier			
1.1	Industrial energy	Nearby electrical substation		
1.2	Backup generator set	On ATS Unit		
1.3	UPS para las TIC	On ATS Unit		
1.4	Respaldo de energía para comunicaciones (UPS o baterias) Power backup for communications (UPS or batteries)	On ATS Unit		
2	Communication supplier			
2.1	Radio link communications support	Identify the external provider of each of the communications services you receive		
2.2	Fiber and copper communications support			
2.3	Fixed and mobile telephone and data communications support			
2.4	Satellite communications support			
3	Drinking water and sanitation provider			
3.1	Water and sanitary networks			
4	Air conditioning system maintenance			
4.1	Centralized climate system			
4.2	Backup climate system for critical rooms			
5	Building Systems Maintenance (BMS)			
5.1	Automatic Fire Detection System (SADI	Identify the external provider of each of the services you receive		
5.2	Fire extinguishing system			
5.3	Access control and CCTV system			
5.4	Intruder protection systems			
5.5	Energy management systems (lighting and climate)			

	Other event categories	Probability Assessment	Impact assessment
1	Environmental events		
1.1	Floods		
1.2	Earthquakes		
1.3	Explosions in the vicinity or on the facility		
1.4	Exposure to chemical contamination		
2	Events affecting the workforce		
2.1	Water and food supply		
2.2	Digestive contamination		
2.3	Strikes		
2.4	Epidemics		
3	Security-related events		
3.1	Hacking		
3.2	Sabotage		
3.3	Terrorism		
4	Air threats		
4.1	Aircraft accident in the vicinity or on the facility itself		
4.2	Attacks on the facility (war scenario)		

Thank You!

ICAO