Who we are?

Egis is an international group offering engineering, consulting, project structuring and operations services (more than 12 000 people worldwide)

Egis Avia is the subsidiary of Egis specialized in Aviation (180 specialists located in Paris and Toulouse)

- Egis Avia offers, engineering, consulting services and training in the fields of:
  - Airports (master planning, design, works supervision & control, consulting)
  - Air Traffic Management (strategy, performance, airspace design, safety…)
  - Air operations (Technical Assistance to Civil Aviation Authorities, Human Factors…)
Egis Avia & safety

- Gap analysis, training and technical assistance for **State Safety Program** improvement

- Support to **SMS** implementation for providers

- Analysis of changes (safety case):
  - For a new Tower, a new system
  - For a new airspace design or a new flight procedure
  - Before important works at an airport

- Among our main references in these fields:
  - DSNA: the French Air Navigation Service Provider
  - EUROCONTROL
  - European Commission & CLEANSKY JU
  - French & African airports
  - Equatorial Guinea, Madagascar, China
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
</tr>
<tr>
<td>B</td>
</tr>
<tr>
<td>C</td>
</tr>
<tr>
<td>D</td>
</tr>
<tr>
<td>E</td>
</tr>
<tr>
<td>F</td>
</tr>
<tr>
<td>G</td>
</tr>
<tr>
<td>H</td>
</tr>
<tr>
<td>I</td>
</tr>
<tr>
<td>J</td>
</tr>
</tbody>
</table>
Introduction
Introduction

Why doing safety?
- To avoid dangerous situations
- To react appropriately to dangerous situations
- To prevent incidents and above all accidents

Annex 19 « safety management » of ICAO defines in appendix 2 (Framework for a SMS) the requirement, for the service provider:
- To develop and maintain a process of identification of the changes that could affect the safety level of his product and services
- And to identify and manage the safety risk associated to these changes

In Europe, rule CE No 2096/2005 requires, before any change in ATM system, to perform a safety study including:
- The identification of hazards
- And then, the evaluation and mitigation of the risks

This study must be carried out by the Air Navigation service Provider.
Introduction

This presentation explains how French ANSP (DSNA) complies with this requirement of safety analysis.

The approach implemented by DSNA consists in performing safety analysis covering:

- The entire life cycle of the considered ATM system, from initial phases to implementation, including maintenance phases and decommissioning,

- The three elements of the ATM system (human factors, procedures and equipment) and their interactions,

- The ground and air components (including spatial component) of the ATM system, through a cooperation with appropriate organization.

This approach particularly concerns modifications of Air Traffic Management procedures.

This approach derives from EUROCONTROL methodology (SAM), herself derived from ICAO.
ATM system
The ATM system

The ATM system, as defined by Eurocontrol

However, changes in ATM system are analysed in their operational environment
The ATM system

The system to be considered therefore includes a wider number of components:
Definition and concept

- Definition of safety analysis
- Hazards
- Mitigation means
- Severity and probability of occurrence
- Risk Tolerability
- Safety Objectives
Definition of safety analysis

Safety analysis refers to:

- A set of activities aiming at evaluating and mitigating risks associated to ATM system changes and at justifying their acceptability.
- A set of documents gathering the results of these activities.

Safety analysis aims at managing hazards by means of mitigations means. It aims at maintaining the safety level during the whole life cycle through safety assurance based on means of safety.
Hazards

Danger affecting the ATM service provision, expressed as close as possible to the main actors. It is an undesirable event regarding the ATM service provision that could cause an accident.

An hazard can be due to technical, procedural or even human aspects.
Mitigation Means

In order to manage the risk, mitigation means are implemented:

- To reduce the probability of occurrence of an hazard (prevention mitigation means) or to reduce the consequences of an hazard (protection mitigation means).
- They can be from technical, procedural or human nature.
- A mitigation mean is evaluated with regards to the risk that it should mitigate. Its quality must be evaluated with regards to its immediacy and to its efficiency.
Severity and probability of occurrence

A risk associated to a hazard is characterized by:

**A severity**: Expresses the impact of the hazard on flight safety (combination of loss of separation and ability to recover the situation). These impacts are assessed on:

- Flight crew and controllers (workload…)
- Functional capabilities of ground and airborne systems
- Ability to provide air traffic management services safely

**A probability of occurrence**: Frequency or probability of occurrence of the hazards, that means the number of time it could
Severity and probability of occurrence

**Prevention mitigation means**
- Modify the combination of failures leading to the hazard →
- Reduce the probability of occurrence of the hazard

**Protection mitigation means**
- Reduce the severity by reducing the impact of the consequences on the operations
  - Some mitigation means have an immediate effect, others have differed
Severity

The evaluation of the severity of an hazard is carried out by considering:

- The **worst credible case** in the considered operational environment
- All the acceptable **protection mitigation means**

The evaluation of the severity of an hazard is carried out with a **qualitative** approach based on the experience of the users (pilots, controllers)
The probability of occurrence can be established according to two approaches:

- Quantitative approach
- Qualitative approach

Quantitative approach:

- Adapted to a technical hazard, that means an hazard associated to an equipment
- Probability of occurrence is evaluated by “service operational hour (SOH)”, according to 5 intervals:
  - Probability of occurrence is more than $10^{-4}$ / SOH
  - Probability of occurrence is between $10^{-4}$ et $10^{-5}$ / SOH
  - Probability of occurrence is between $10^{-5}$ et $10^{-6}$ / SOH
  - Probability of occurrence is between $10^{-6}$ et $10^{-8}$ / SOH
  - Probability of occurrence is less than $10^{-8}$ / SOH
Probability of occurrence

Qualitative approach:

- Adapted to a non-technical hazard, like implementation of new procedures or new working method
- The probability is an estimation, making sense from an operational point of view
  - **Extremely improbable**: can occur one time every 1000 years in an ATC organism (never happened in the ATC organism) \(10^{-7}\) / operation hour
  - **Improbable**: can occur one time every 5 or 10 years in an ATC organism \(10^{-5}\) / operation hour
  - **Occasional**: 1 or 2 times a year in an ATC organism \(10^{-4}\) / operation hour
  - **Frequent**: Many times a year in an ATC organism \(10^{-3}\) / operation hour
  - **Very frequent**: Many times a month in an ATC organism \(10^{-2}\) / operation hour
Risk Tolerability

Risk tolerability relies on the **combination** of the probability of occurrence and the severity of the **worst credible case**

<table>
<thead>
<tr>
<th></th>
<th>Very frequent</th>
<th>Frequent</th>
<th>Occasional</th>
<th>Improbable</th>
<th>Extremely improbable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazardous</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negligible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*technical hazards*

**Grey Area** corresponds to **not tolerable risk**

Source: DSNA
Safety objectives

The safety objectives define the maximum probability of occurrence of an hazard, in order to ensure the tolerability of the risk, based on a risk tolerability matrix.

The achievement of the safety objectives relies on:

- **Assumptions**: Protection or prevention mitigation means already included in regulation documents.
- **Requirements**: New protection or prevention mitigation means required to reach the safety objective.
Methodology

- General methodology
- Before starting the safety analysis...
General methodology

NA methodology for the safety analysis relies on Eurocontrol’s SAM (Safety Assessment Methodology) including three phases:

1. **FHA** (*Functional Hazard Assessment*): Risk evaluation

2. **PSSA** (*Preliminary System Safety Assessment*): Risk mitigation strategy

3. **SSA** (*System Safety Assessment*): Demonstration of the implementation of the risk mitigation strategy
Before starting the safety analysis...

It is important to describe the environment and the change in order to identify the scope of the safety analysis.

The scope of the safety analysis can be different from the.

The scope of the safety analysis can be different from the.

The scope of the safety analysis can be different from the.

The scope of the safety analysis can be different from the.

The scope of the safety analysis can be different from the.

The scope of the safety analysis can be different from the.
Before starting the safety analysis…

This description can be established following an operational (actions) or functional (functions) model, and must allow to identify:

- Operational context
- Actors involved in the change (before, during and after)
- Interfaces with external systems
- Different operational functions or actions characterising the change

This technical description allows the definition of assumptions that will be considered as mitigation means.
Safety Analysis

- Safety case: FHA, PSSA, SSA
- « EPIS CA »
- Dossier vs. EPIS
Risk evaluation (FHA)

1- FAILURE MODES IDENTIFICATION

What can fail on every function / action?

Loss of degradation of system functions

2- HAZARDS IDENTIFICATION

What are the potential consequences?

Potential impacts on the safety

3- HAZARDS EVALUATION

What are the severities of these consequences?

Contribution to collision risk
Risk Mitigation Strategy (PSSA)

1- CAUSES IDENTIFICATION

What are the combination of causes (failure) leading to the hazard?

2- APPORTIONMENT OF SAFETY OBJECTIVES

How allocating the safety objective on the causes?

3- IDENTIFICATION OF PREVENTION MITIGATION MEANS

How reaching the safety objectives?

---

Human or technical failure

Apportionement of the safety objective on the different components of the change

Implementation of new equipment, procedure or working methods
System safety assessment (SSA)

- Demonstrate that the system, as implemented and operated, satisfy all the allocated safety requirements and comply durably with the safety objectives.

1- SAFETY ASSESSMENT

Are the assumptions and safety requirements reached?

Documentation update, rules...

2- TRANSITION PHASES ANALYSIS

Have mitigations means been defined in order to manage risk during transition phases?

NOTAM, maintenance procedures....

3- DETERMINATION OF...
Objective 1: Determine the necessity to perform a complete safety case
Objective 2: Conduct the safety analysis associated to the change

Covered by the EPIS through « Characterisation of the change and the risk »

Covered by the EPIS through « Hazards detailed analysis »

Specific sections to be fulfilled by the ANSP
When choosing a safety case?

- In case of wide changes
- In case of changes in constraining environment
- According to the results of the EPIS
- When the change requires the implementation of new aeronautics standards

Objectives of the safety case:

- Provide a more detailed analysis than the one performed in an
Introduction to generic EPIS CA RNAV
Introduction to generic EPIS CA RNAV

Three RNAV generic safety analysis developed by DTI:

- EPIS CA RNAV GNSS (LNAV, LNAV/VNAV et LPV) based on the generic safety case
- EPIS CA SID RNAV 1 (radar and non radar)
- EPIS CA STAR and approach INI and ITM RNAV 1 (radar and non radar)

Why producing these EPIS CA?

- To facilitate the implementation of new procedures locally
- To present, with an easily accessible format, the result of generic safety analysis (knowing that the severity of the operation is compatible with EPIS CA formalism)
Scope of the RNAV GNSS analysis
Operational context RNAV GNSS

GPS

Signal EGNOS+GPS

Airborne Systems

Operator/pilot:
Operational procedures
Airborne certification

Legal Recording

Database provider: procedure coding
Operator: Ground integration of the procedure

NAV

RNAV GNSS Phraseology

ATC Procedures

Procedure design
Flight test
Procedure publication
Scope and assumptions of the RNAV GNSS analysis

The analysis (cause identification, prevention mitigation means definition...) is carried out on every phases of flight:

- Pre-operation
- Pre-flight
- Before starting the approach – before IAF
- Before initial approach: IAF to IF
- Intermediate approach: IF to FAP
- Final approach: final segment
- Missed approach procedure – First segment

Assumptions regarding the environment and the different actors are defined:

- For reminder only because they are already mentioned in regulation documents
Scope of the SID RNAV 1 analysis

Last point on the SID = name of the SID
Operational context SID RNAV1

Database provider: procedure coding
Operator: Ground integration of the procedure

Operator/pilot: Operational procedures Airborne certification

GPS
DME
NAV
Airborne System
RNAV Phraseology
ATC Procedures
SIA: NOTA (preflight)
Scope and assumptions of the SID RNAV 1 analysis

The analysis (cause identification, prevention mitigation means definition...) is carried out on every phases of flight:

- Pre-operation
- Pre-flight
- Before departure – before DER
- From DER to connexion with En Route network

Assumptions regarding the environment and the different actors are defined:

- Assumption under the responsibility of DSNA must be verified
EPIS CA STAR RNAV1
Scope of the STAR RNAV 1 analysis

First point of the STAR = name of the STAR
Operational context STAR RNAV1

GPS

Operator/pilot:
Operational procedures + Airborne certification

DME

Database provider:
Procedure coding
Operator: Airborne integration of the database

Airborne systems

Legal recording

RNAV phraseology

ATC procedures

NOTAM
Scope and assumptions of the STAR RNAV 1 analysis

The analysis (cause identification, prevention mitigation means definition...) is carried out on every phases of flight:

- Pre-operation
- Pre-flight
- Before arrival – before the first point of the STAR to I’IAF
- From IAF to FAF/FAP

Assumptions regarding the environment and the different actors are defined:

- Assumption under the responsibility of DSNA must be verified
Conclusion
Conclusion

Safety studies through an EPIS CA or a complete safety case rely on the same methodology:

- System analysis and risk identification
- Risk evaluation based on the analysis of the consequences and the causes
- Identification of assumptions and requirements reducing the risk to an acceptable level
- Identification of means ensuring the implementation of the assumptions and requirements for the operational implementation of the system and durably

Safety analysis requires to be supported by technical and operational experts in position to evaluate the risks.

Safety analysis must be launched as soon as possible because it can impact others activities of the project (for example procedure...
Conclusion

These 3 EPIS CA RNAV rely on common hazards but with specific differences for each operation, identified all along the EPIS.

Regarding **PBN procedure design**, attention is drawn on:

- Quality process applied by designers (verification/validation/traceability)
- Naming of the charts and consistency with phraseology
- Differentiation with convensional procedures
- Life cycle management of the FAS DB for LPV
- Critical DME management for RNAV1

These generic EPIS CA RNAV constitute a support to the organisms implementing operation but, they do not replace the exhaustive analysis that must be performed by these organisms.
Contact
Anne-Laure VOGEL
anne-laure.vogel@egis.fr
Tel: +33 5 16 57 00 61
Mob: +33 6 46 44 88 76
Safety case process

EPIS

Safety Plan:
- Description of the change, perimeter of the analysis and assumptions
- Organisation: participants, roles, responsibilities, ...
- Planning
- Planned methodology (Qualitative, fault trees, ...),
- Planned analysis, tests...

Safety case

Operational implementation of the change

Safety assurance:
- to keep an analysis up-to-date in case of modification of the planned intervention