Safety Case

Foreword

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

Contents

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.

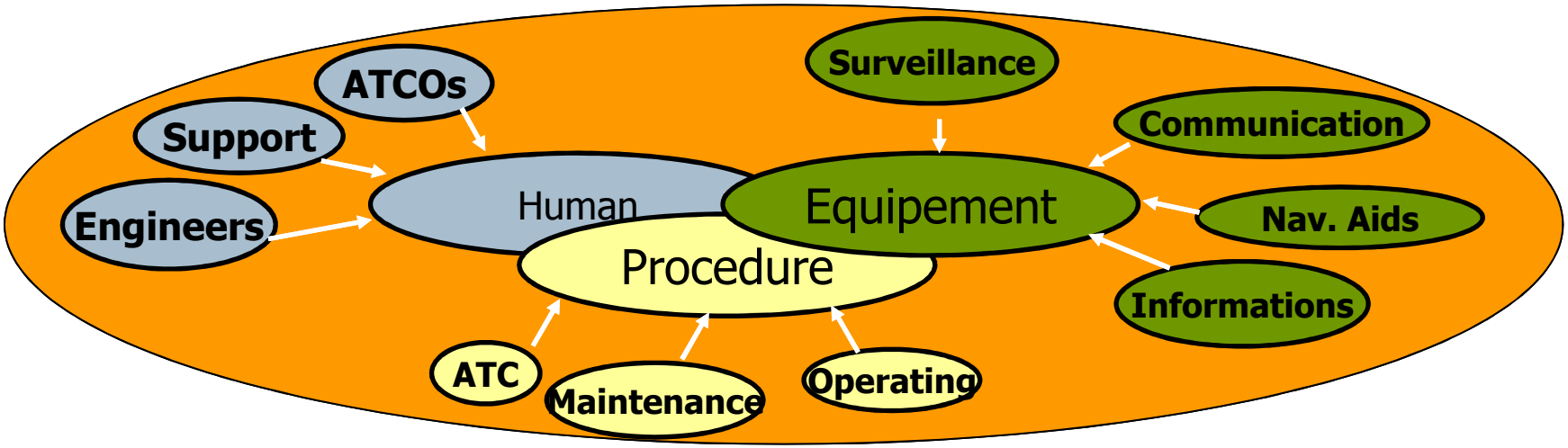
This approach particularly concerns modifications of Air Traffic Management procedures

This approach derives from EUROCONTROL methodology (SAM), herself derived from ICAO

ATM system

The ATM system

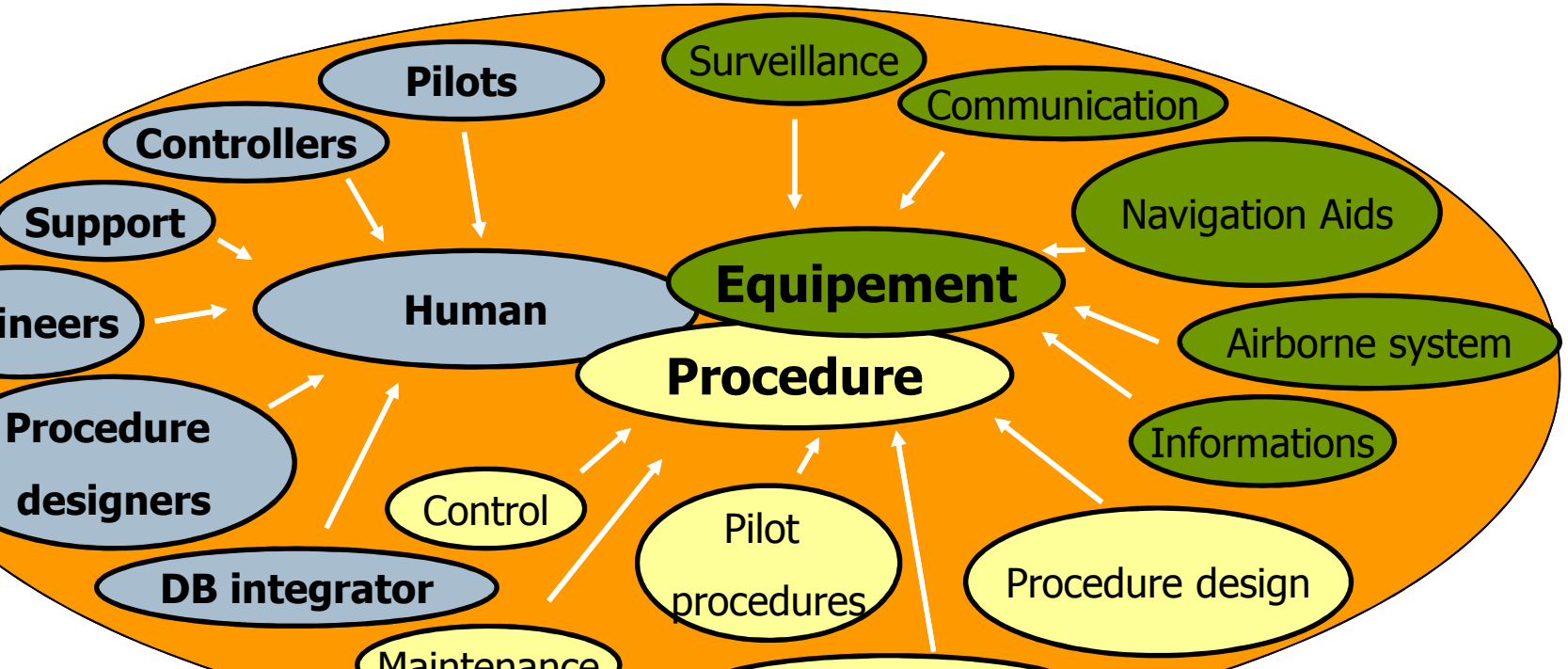
The ATM system, as defined by Eurocontrol



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

The ATM system

e system to be considered therefore includes a wider
number of components :



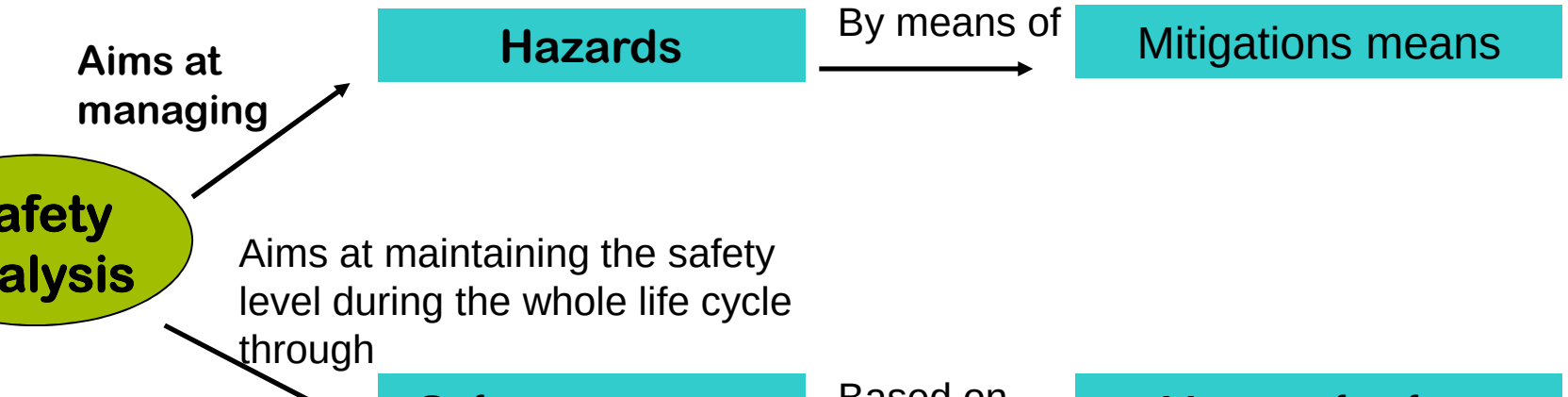
Definition and concept

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

Definition of safety analysis

afety 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



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

order to manage the risk, **mitigation means** are mplemented :

- 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

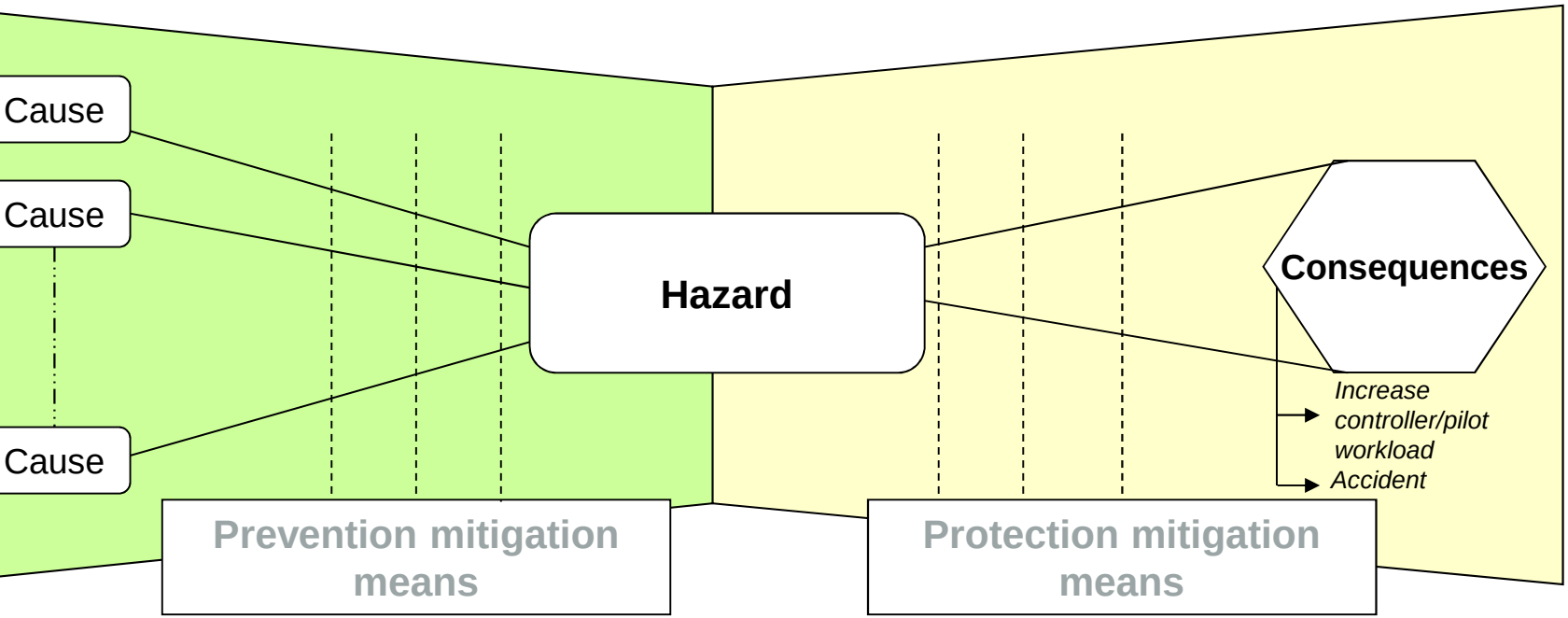
risk associated to an hazard is characterized by :

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



Modify the combination of failures leading to the hazard →
Reduce the probability of occurrence of the hazard

Reduce the severity by reducing the impact of the consequences on the operations
Some mitigation means have an

Severity

e 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**

e evaluation of the severity of an hazard is carried out with a **qualitative** approach based on the experience of the users (pilots, controllers)

Probability of occurence

e probability of occurrence can be established
according to two approaches :

- Quantitative approach
- Qualitative approach

uantitative 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 occurence

ualitative approach:

- Adapted to a non-technical hazard, like implementation of new procedures or new working method
- The probability is a estimation, making sense from an operational point of view
  - ***Extremely improbable*** *:* can occur one time every 1000 year 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} /

Risk Tolerability

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

	Very frequent	Frequent	Occasional	Improbable	Extremely improbable
atastrophic					
azardous					
ajor					
inor					
egligible					

Source: DSNA

technical hazards

y Area corresponds to **not tolerable risk**

Safety objectives

e safety objectives define the **maximum robability of occurrence of an hazard**, in order o ensure the **tolerability** of the risk, based on a risk olerability matrix.

e 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

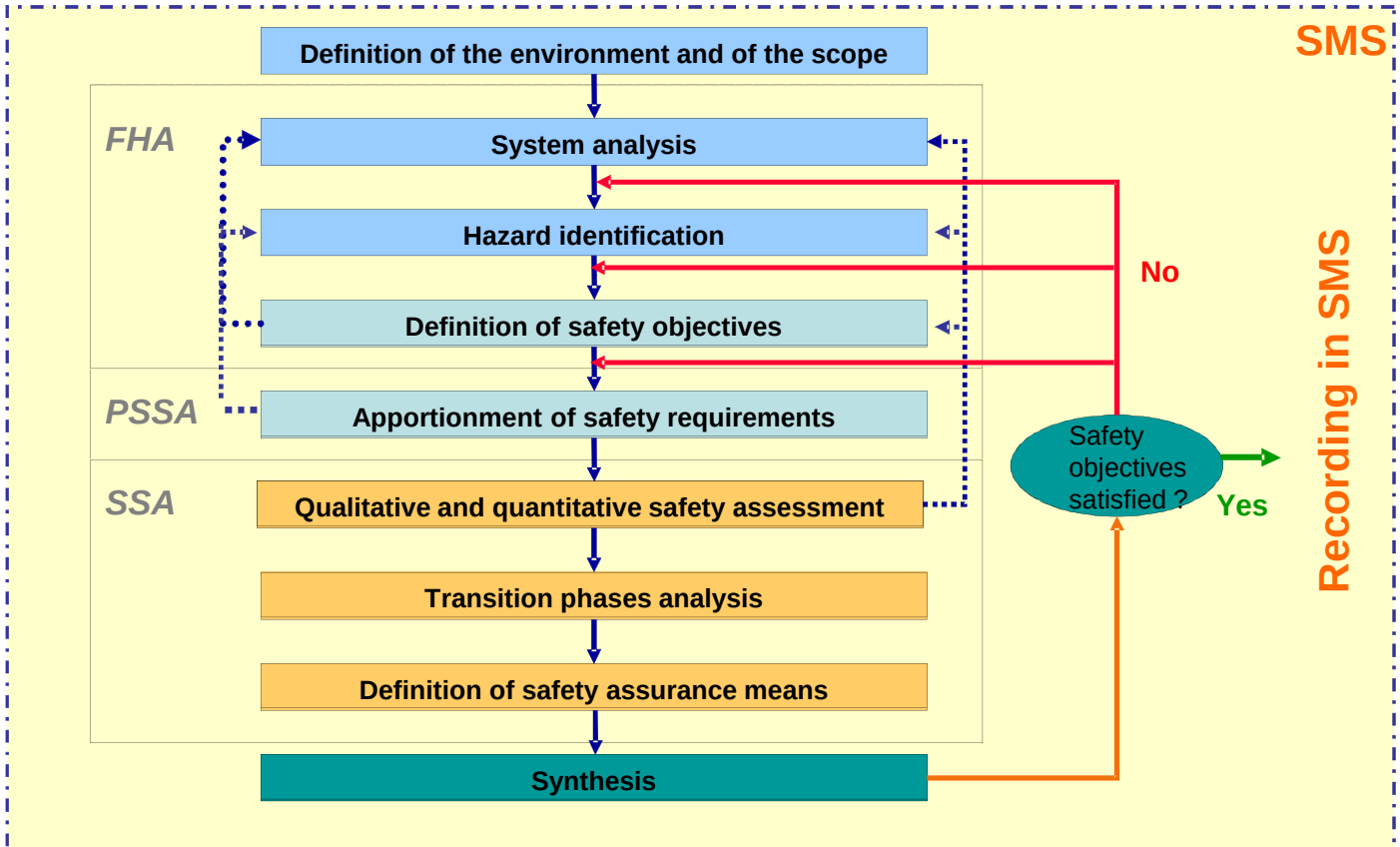
- General methodology
- Before starting the safety analysis…

General methodology

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

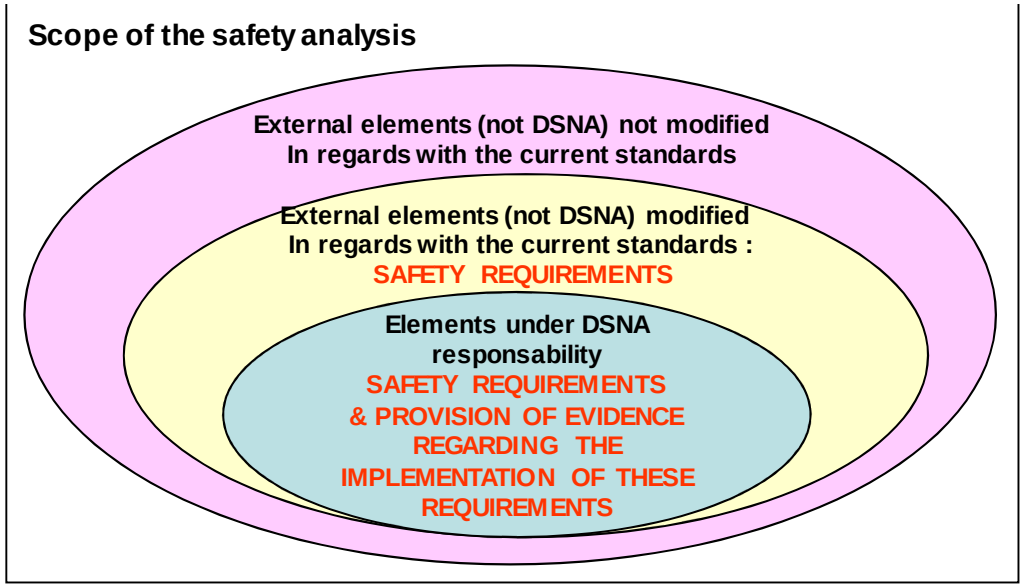
1. **FHA** (*Functional Hazard Assessment): Risk evaluation*
2. **PSSA** (*Preliminary System Safety Assessment): Risk mitigation strategy*
3. **SSA** (*System Safety Assessment): Demonstration of the implementation of the risk mitigation strategy*

General methodology



Before starting the safety analysis…

s important to describe the environment and the change in
order to identify the scope of the safety analysis



e scope of the safety analysis can be different from the

Before starting the safety analysis…

is 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

is technical description allows the definition of **assumptions that will be considered as mitigation means**

Safety Analysis

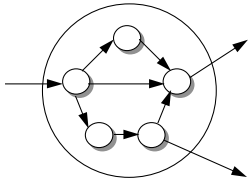
- Safety case : FHA, PSSA, SSA
- « EPIS CA »
- Dossier vs. EPIS

Risk evaluation (FHA)

1- FAILURE MODES IDENTIFICATION

What can fail on every function / action ?

Loss of degradation of system functions



2- HAZARDS IDENTIFICATION

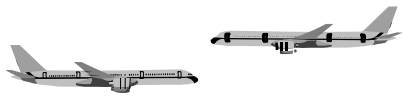
What are the potential consequences ?

Potential impacts on the safety

3- HAZARDS EVALUATION

What are the severities of these consequences ?

Contribution to collision risk



WHICH SAFETY LEVEL MUST BE

Risk Mitigation Strategy (PSSA)

1- CAUSES IDENTIFICATION

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

Human or technical failure

2- APPORTIONMENT OF SAFETY OBJECTIVES

How allocating the safety objective on the causes ?

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

3- IDENTIFICATION OF PREVENTION MITIGATION MEANS

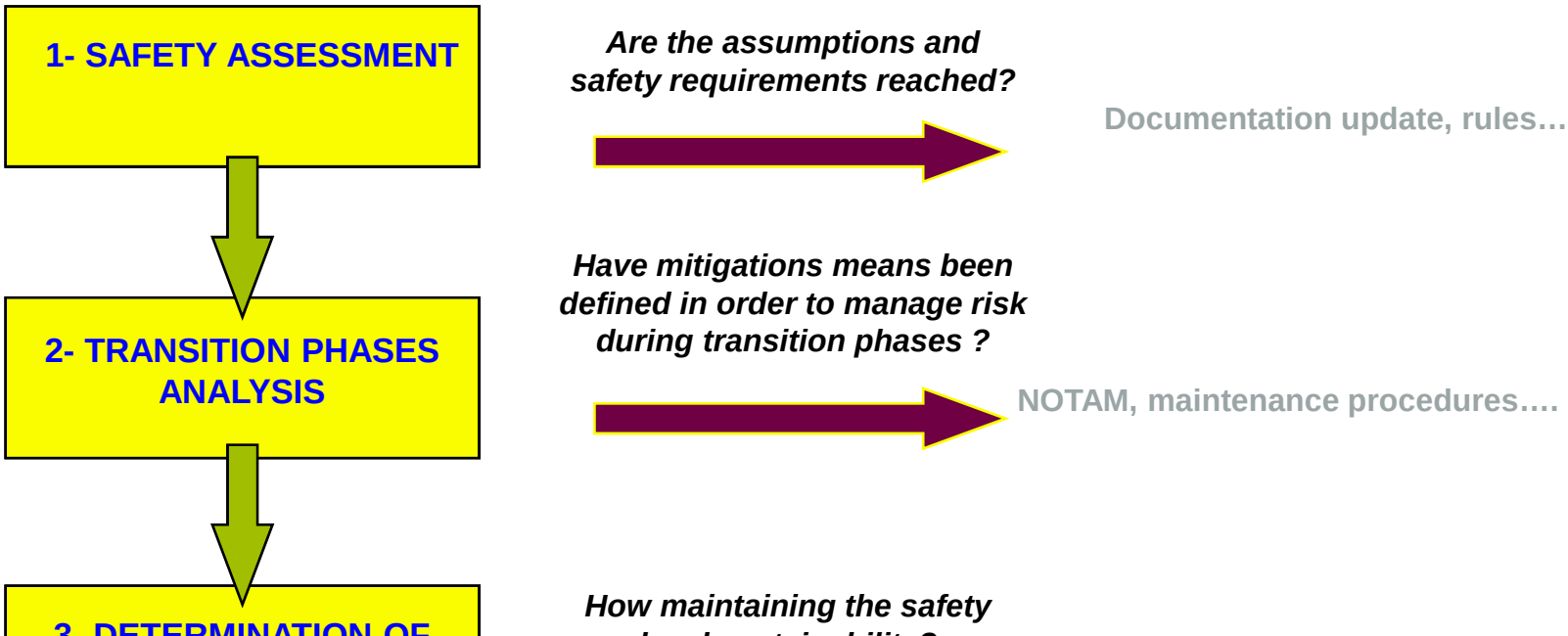
How reaching the safety objectives ?

Implementation of new equipement, procedure or working methods

WICH REQUIREMENTS MUST BE

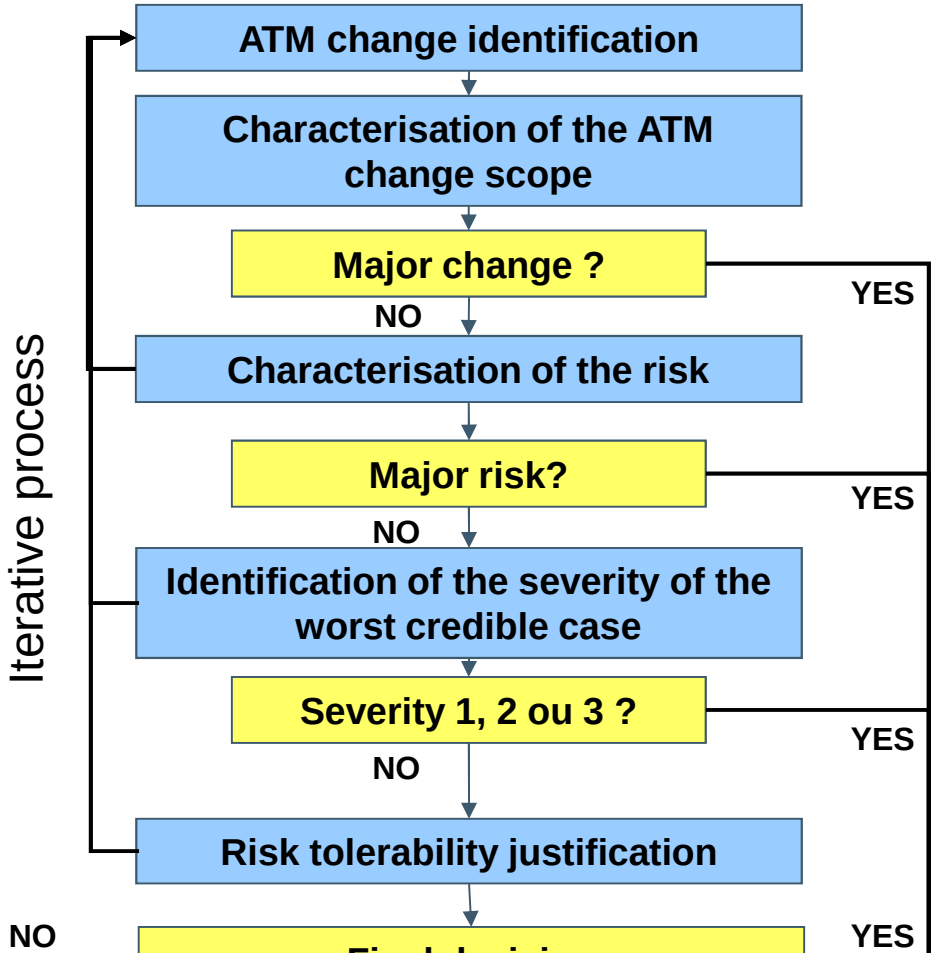
System safety assessment (SSA)

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



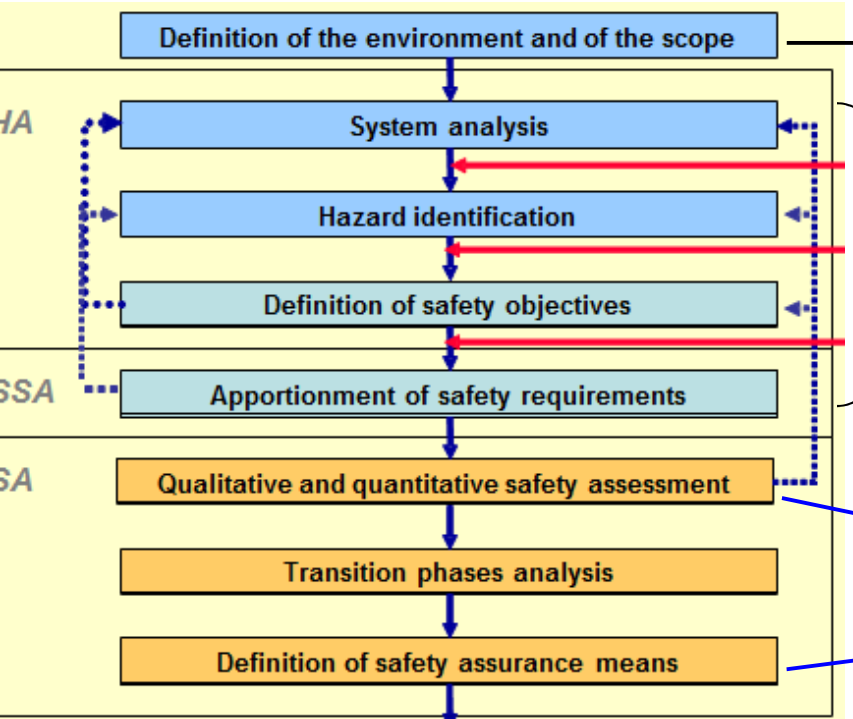
« EPIS CA » process

jective 1:
Determine the
necessity to
perform a complete
safety case



« EPIS CA » process

jective 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

EPIS and safety case

hen 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

bjectives 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

ree RNAV generic safety analysis developed by DTI :

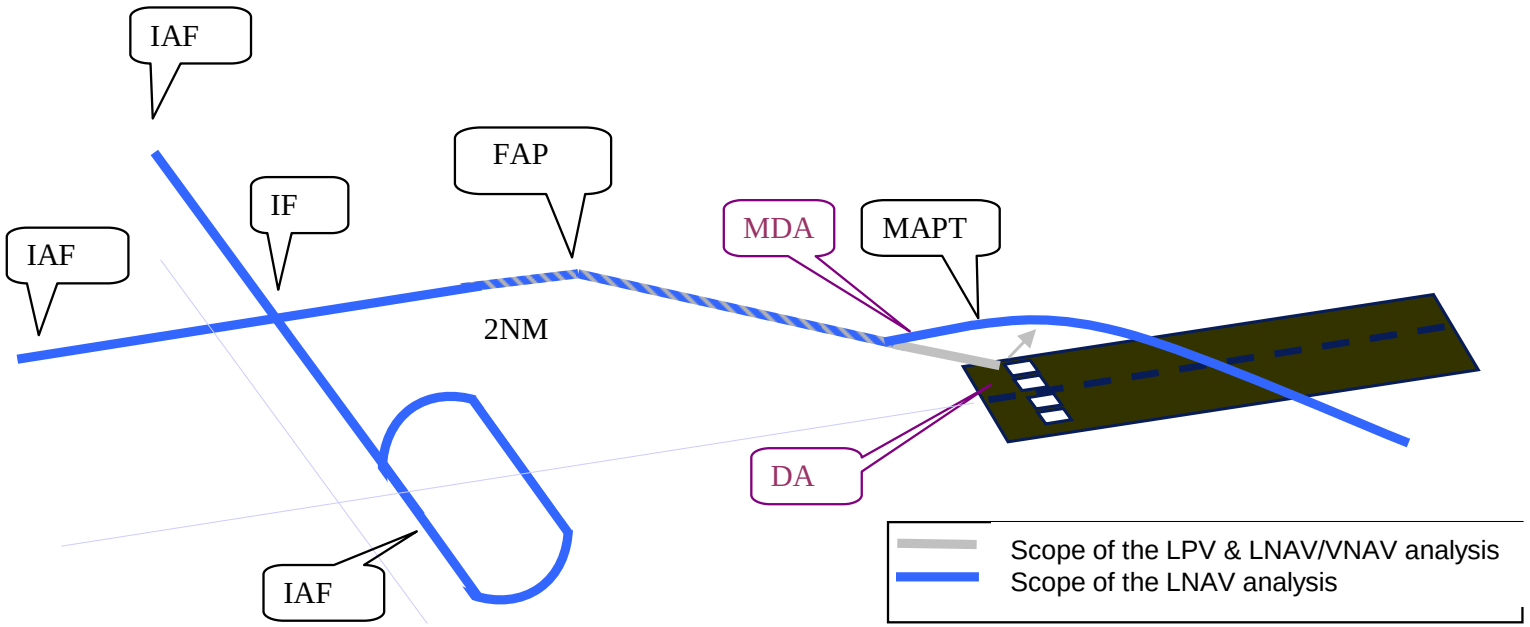
- EPIS CA RNAV GNSS (LNAV, LNAV/VNAV et LPV) based on the generic safety case
- EPIS CA SID RNAV 1 (radar and non radar)
- EPIS CA STAR and approach INI and ITM RNAV 1 (radar and non radar)

ny producing these EPIS CA?

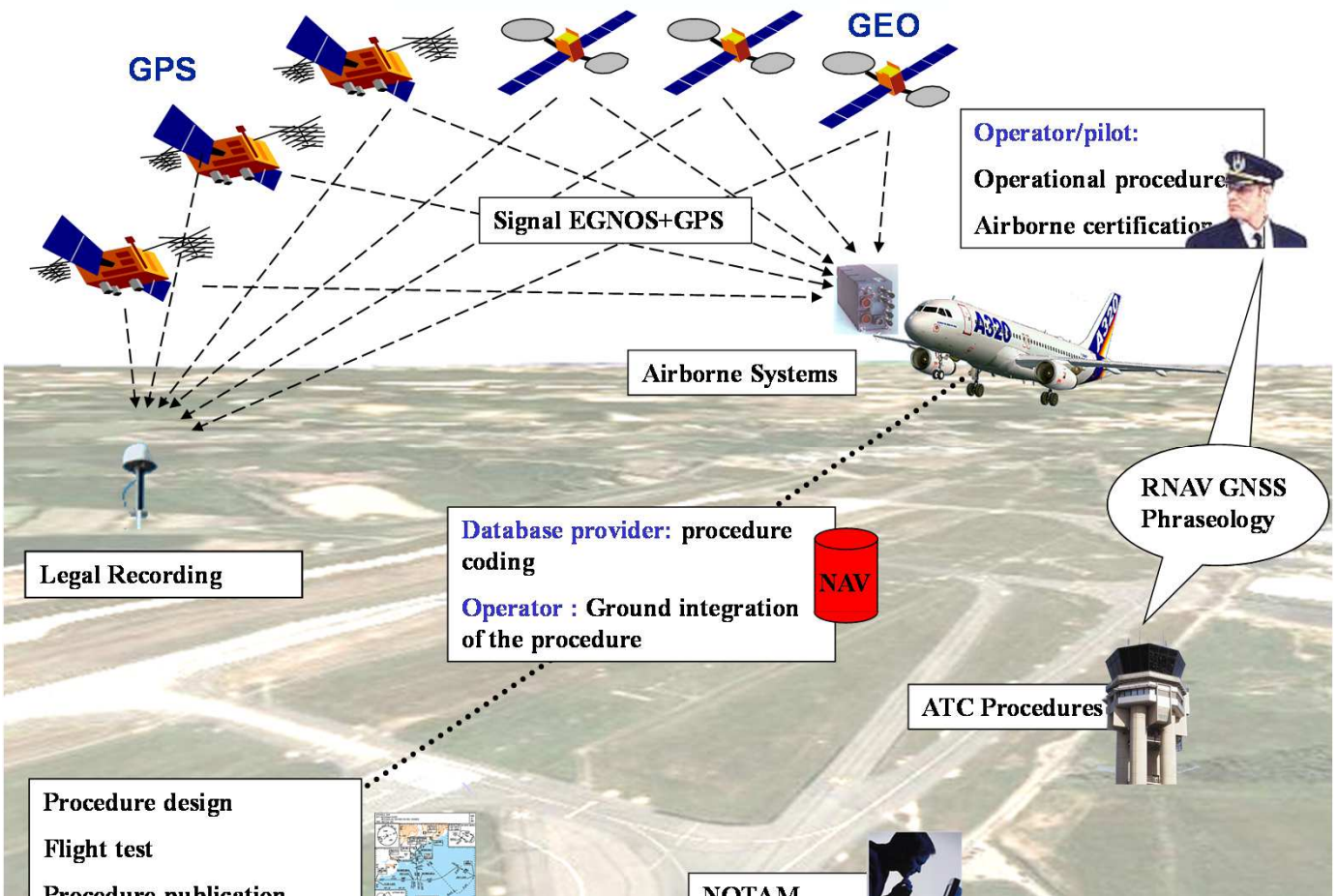
- To facilitate the implementation of new procedures locally
- To present, with an easily accessible format, the result of generic safety analysis (knowing that the severity of the operation is compatible with EPIS CA formalism)

EPIS CA RNAV GNSS

Scope of the RNAV GNSS analysis



Operational context RNAV GNSS



Scope and assumptions of the RNAV GNSS analysis

e analysis (cause identification, prevention mitigation means inition…) is carried out on every phases of flight:

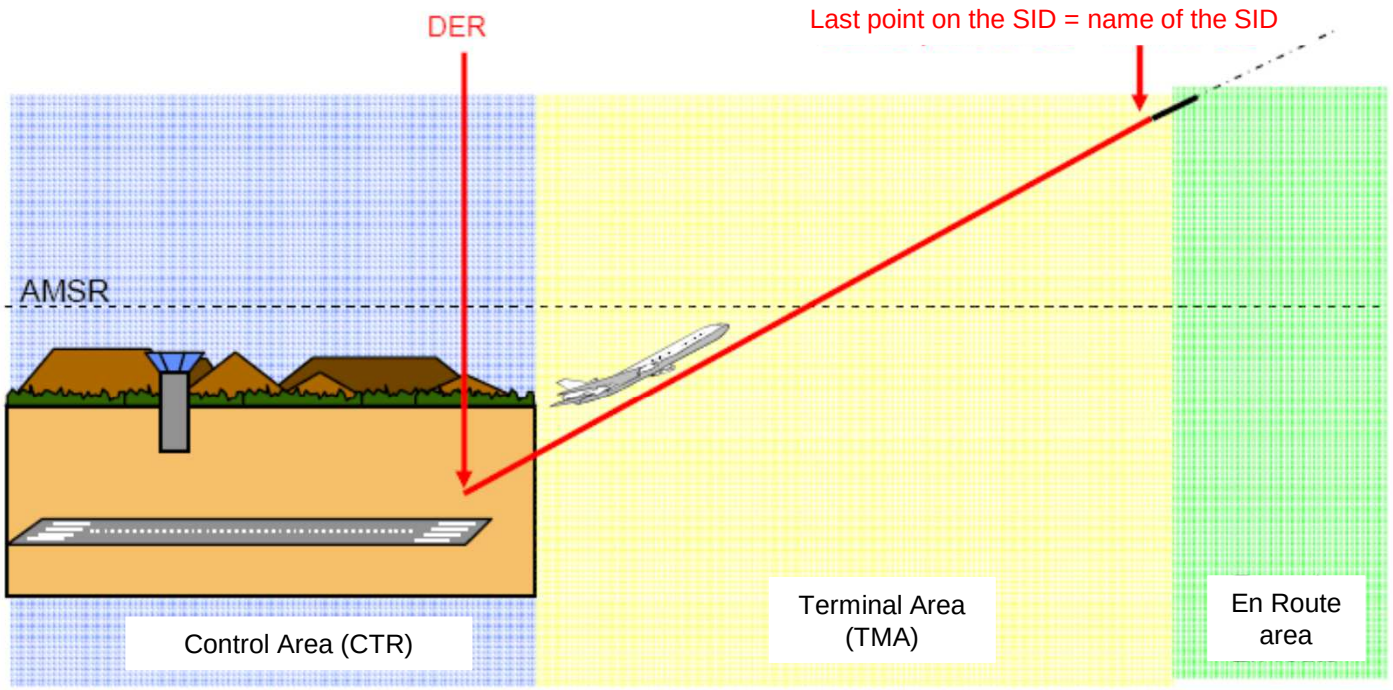
- Pre-operation
- Pre-flight
- Before starting the approach – before IAF
- Before initial approach: IAF to IF
- Intermediate approach: IF to FAP
- Final approach: final segment
- Missed approach procedure – First segment

umptions regarding the environment and the different actors are ined:

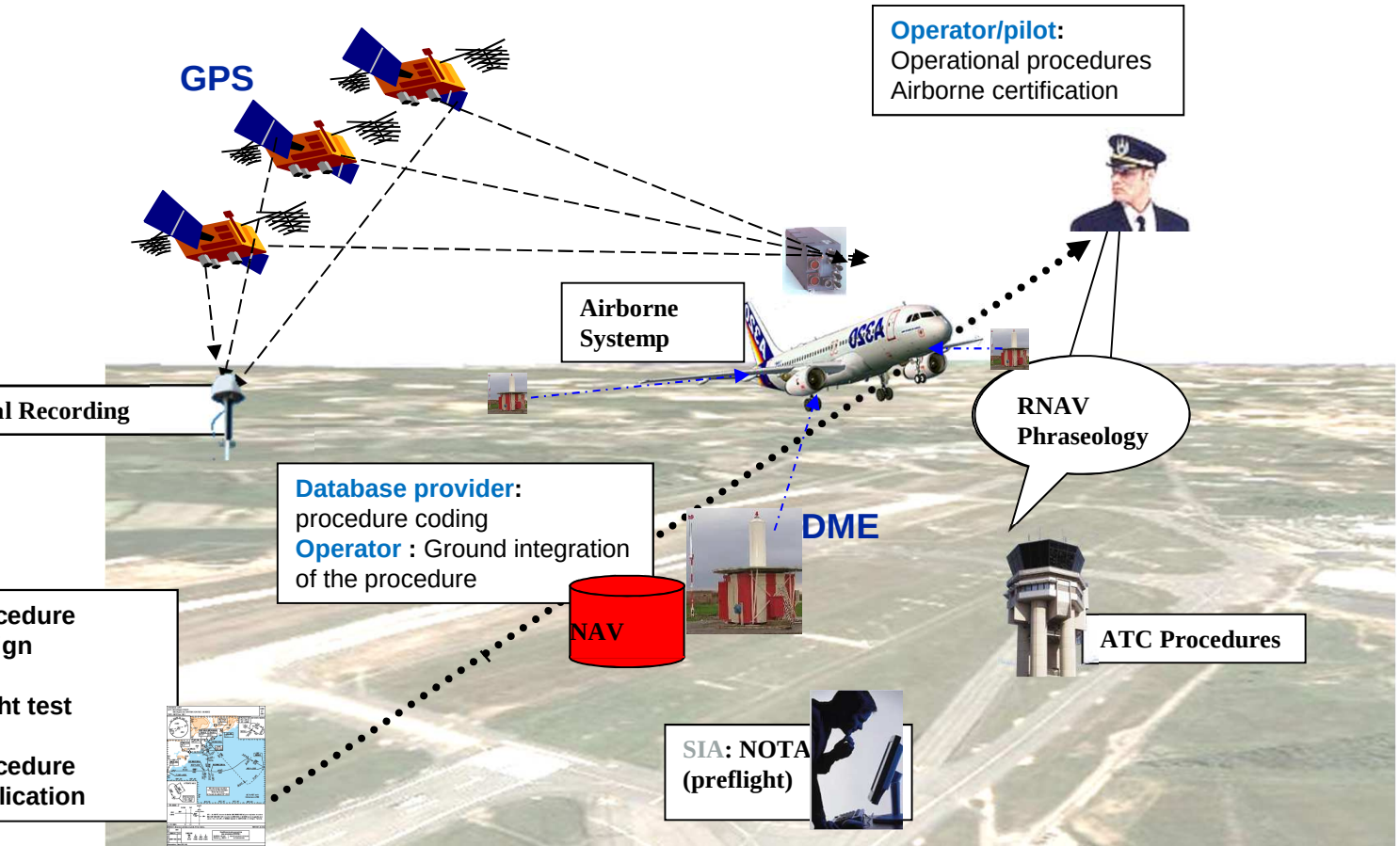
- For reminder only because they are already mentioned in regulation documents

EPIS CA SID RNAV1

Scope of the SID RNAV 1 analysis



Operational context SID RNAV1



Scope and assumptions of the SID RNAV 1 analysis

e analysis (cause identification, prevention mitigation means inition…) is carried out on every phases of flight :

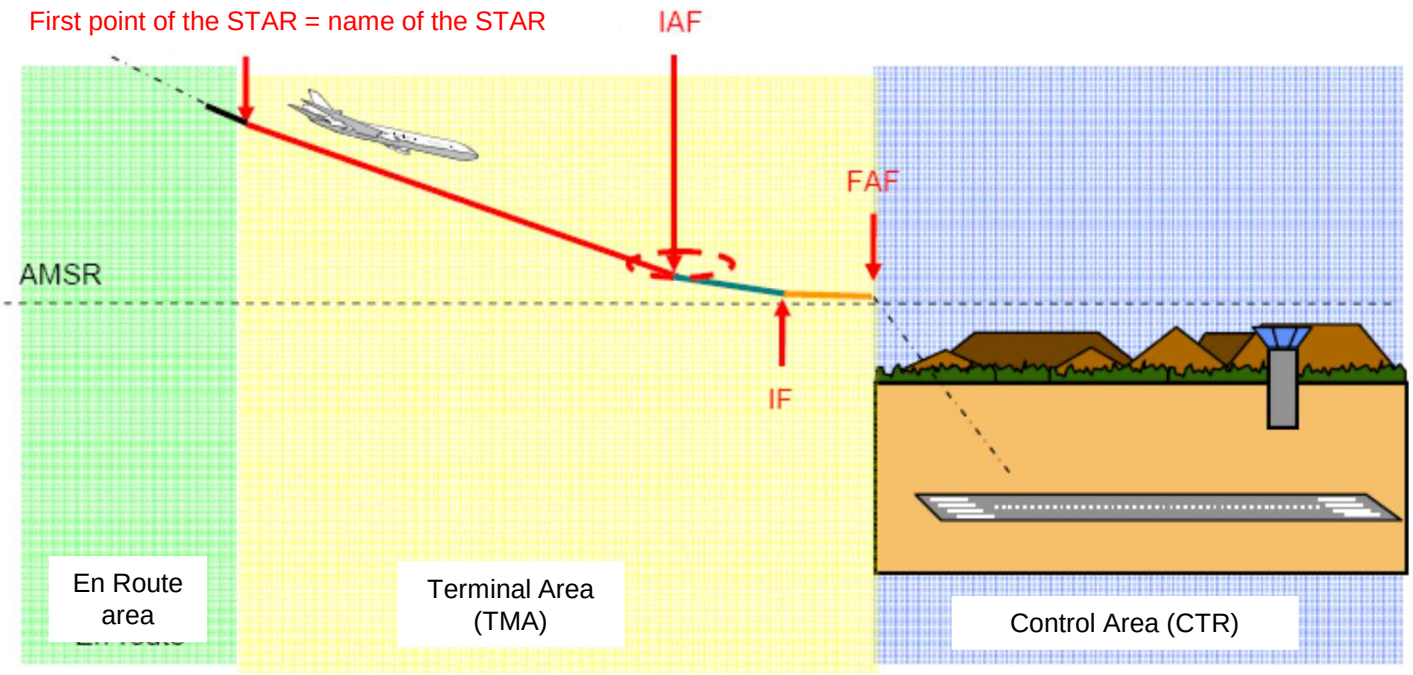
- Pre-operation
- Pre-flight
- Before departure – before DER
- From DER to connexion with En Route network

sumptions regarding the environment and the different ors are defined :

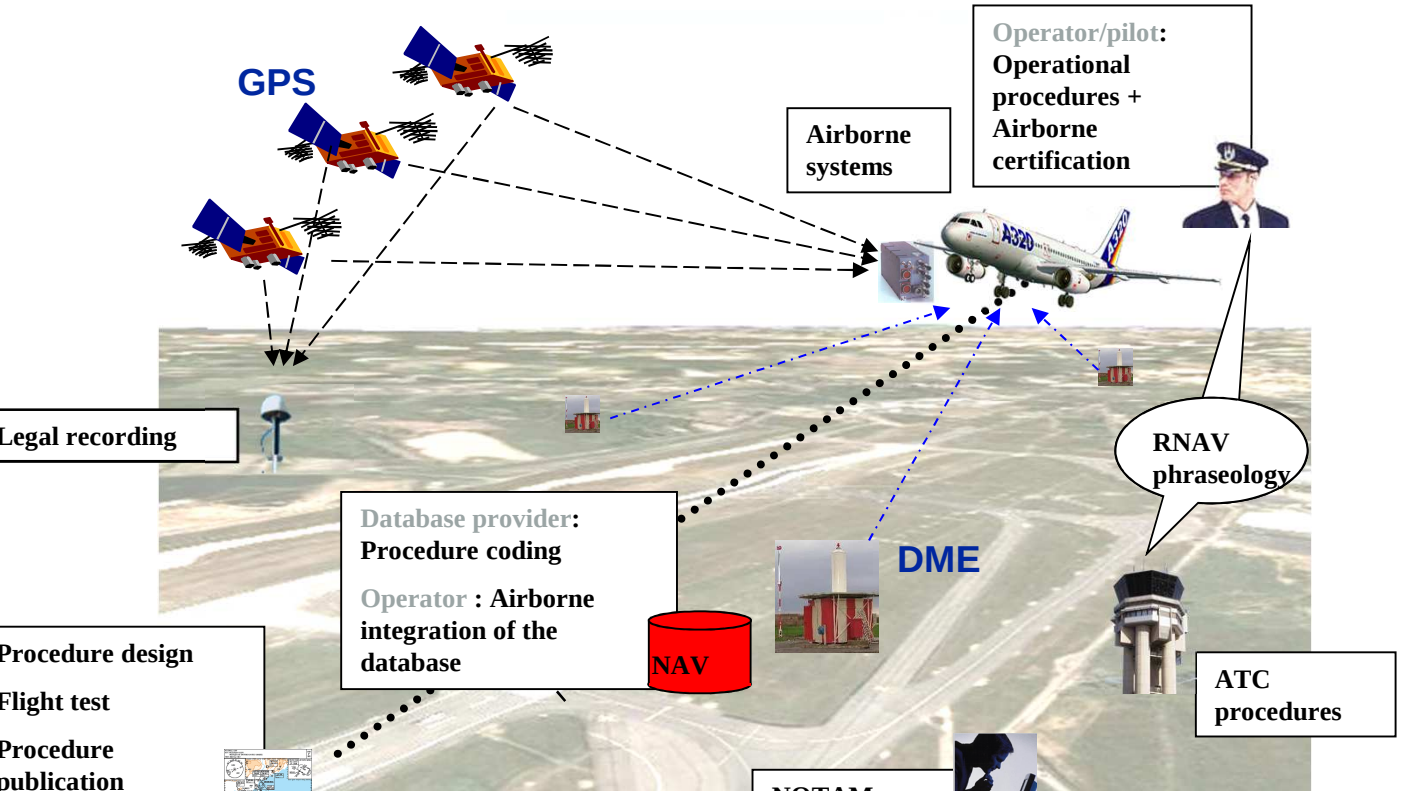
- Assumption under the responsibility of DSNA must be verified

EPIS CA STAR RNAV1

Scope of the STAR RNAV 1 analysis



Operational context STAR RNAV1



Scope and assumptions of the STAR RNAV 1 analysis

e analysis (cause identification, prevention mitigation means inition…) is carried out on every phases of flight :

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

sumptions regarding the environment and the different ors are defined :

- Assumption under the responsibility of DSNA must be verified

Conclusion

Conclusion

ety studies through an EPIS CA or a complete safety case rely on the
ne 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

ety analysis requires to be supported by technical and operational
erts in position to evaluate the risks

fety analysis must be launched as soon as possible because
an impact others activities of the project (for example procedure

Conclusion

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

arding **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 convectional procedures
- Life cycle management of the FAS DB for LPV
- Critical DME management for RNAV1

se generic EPIS CA RNAV constitute a support to the organisms implementing
operation but, they do not replace the **exhaustive analysis** that must be
ormed by these organisms.

Contact

ne-Laure VOGEL
ne-laure.vogel@egis.fr
: +33 5 16 57 00 61
ob: +33 6 46 44 88 76

Safety case process