Implementing EC 482/2008

At NAV Portugal

Paula Santos
paula.santos@nav.pt

Goal

This presentation aims to share the way NAV Portugal is following for the implementation of regulation EC 482/2008, the prerequisites for its implementation, the achievements and the on-going work.

Agenda

Regulatory framework:

- EU 1035/2011
- EC 482/2008
- EC 552/2004

Gap analysis – What is missing for EC 482/2008?

- Quantitative Safety Levels
- Hazards, Safety Objectives (Meaningful, measurable), …
- Functional System Description
- Functional System Architecture

Implementation plan

Communication with NSA

Regulatory framework

Several European regulations are applicable to NAV (and other ANSP), most of them are transversal to the whole organization.

A centralised implementation and monitoring of compliance

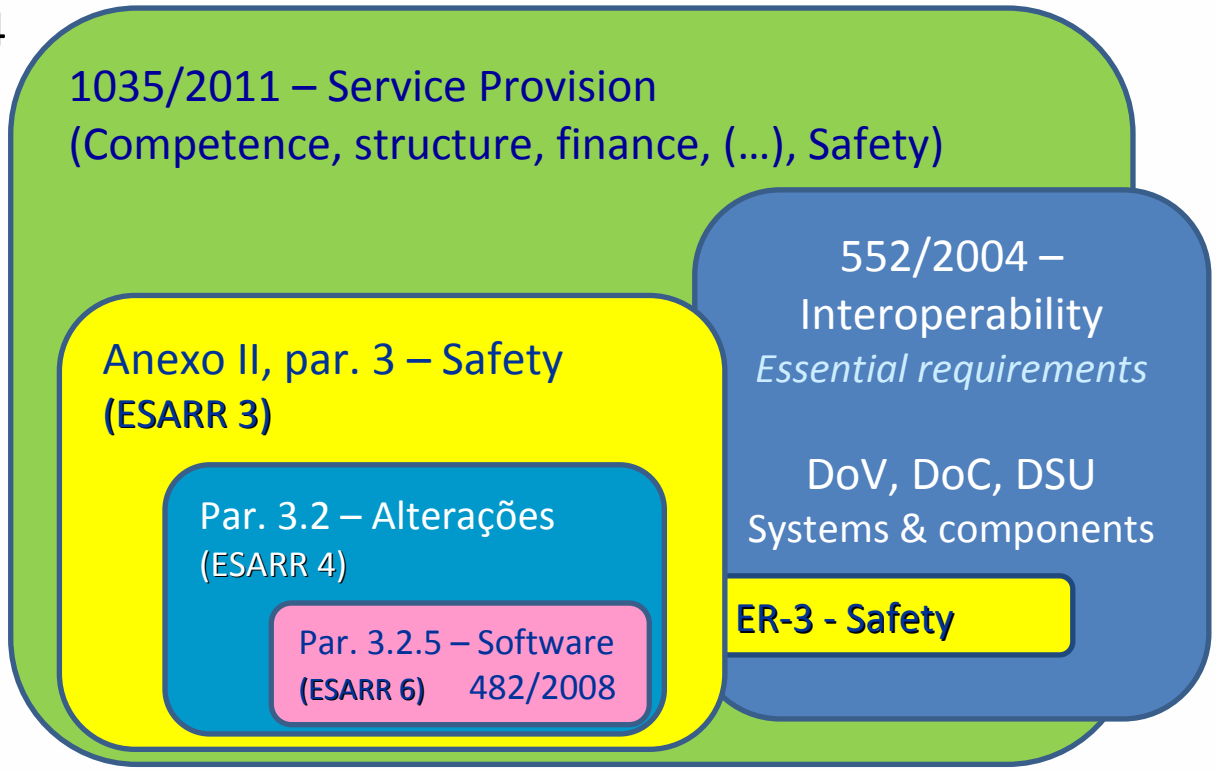
- Eases harmonization and integration of solutions
- Allows a global view of the impact
- Is less prone to failures / gaps

A global view helps a lot…

Regulatory framework

Scope:

- CE 1035/2011
- CE 482/2008
- CE 552/2004



Regulation EC 1035/2011

Article 4
Granting of certificates

1. In order to obtain the certificate necessary to provide air navigation services, and without prejudice to Article 7(5) of Regulation (EC) No 550/2004, organisations shall comply with:

(a)the general requirements for the provision of air navigation services set out in Annex I;
(b)the additional specific requirements set out in Annexes II to V according to the type of service they provide.

COMMISSION IMPLEMENTING REGULATION (EU) No 1035/2011

of 17 October 2011

laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010

Regulation CE 1035/2011

ANNEX II

Specific requirements for the provision of air traffic services

3. SAFETY OF SERVICES

3.1. Safety management system (SMS)

3.1.1. General safety requirements

(…)

3.2.5.

Section 5

Software safety assurance system

Within the operation of the SMS, a provider of air traffic services shall implement a software safety assurance system in accordance with ***Regulation (EC) No 482/2008.***

COMMISSION IMPLEMENTING REGULATION (EU) No 1035/2011

of 17 October 2011

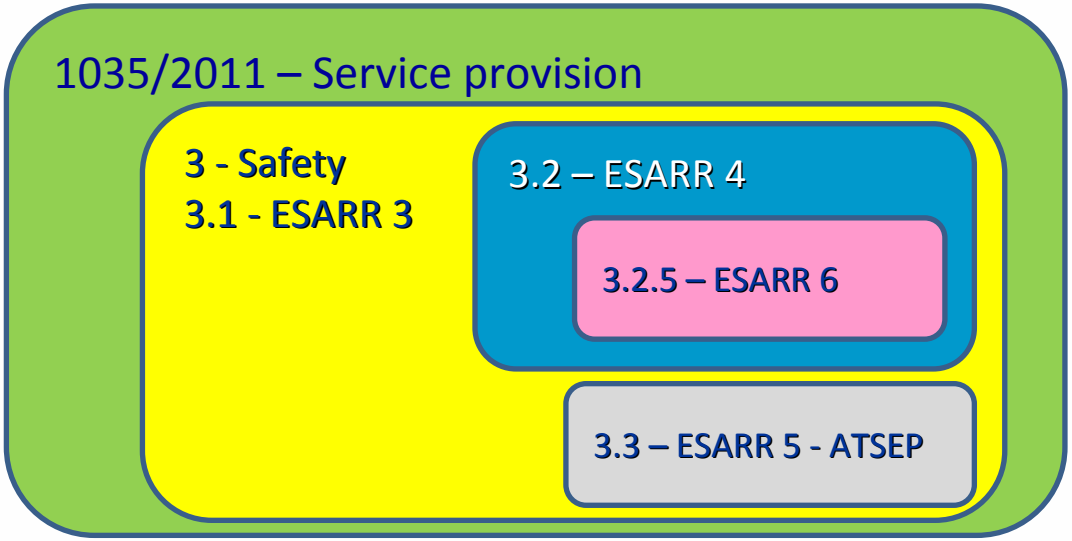
laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010

Regulation EC 1035/2011

Replaces regulation 2096/2005.

Transposes the ESARR to European regulation

- ESARR3 – Safety Management System (SMS) – Annex I, par 3.1
- ESARR4 – Risk assessment and mitigation in ATM (changes) – par 3.2
- ESARR5 – ATM services' personnel– par 3.3 (ATSEP's)
- ESARR6 – Software in ATM Functional Systems (transposed to CE 482/2008) – par 3.2.5



Regulation EU 1035/2011

Annex II
3.2.3 - Section 3
The ***results, associated rationales and evidence*** of the risk assessment and mitigation processes, including hazard identification, ***shall be collated and documented*** in a manner which ensures that:

(a) ***complete arguments*** are established ***to demonstrate that*** the constituent part under consideration, as well as ***the overall ATM functional system are, and will remain tolerably safe by meeting allocated safety objectives and requirements.*** This shall include, as appropriate, specifications of any predictive, monitoring or survey techniques being used;

(b) all safety requirements related to the implementation of a change are ***traceable*** to the intended operations / functions.

Regulation EC 482/2008

Article 3
General safety requirements

1. Whenever an organisation is required to implement a ***risk assessment and mitigation process*** in accordance with applicable Community or national law, ***it shall define and implement a software safety assurance system*** to deal specifically with EATMN software related aspects, including all online software operational changes, and in particular cutover or hot swapping.

COMMISSION REGULATION (EC) No 482/2008

of 30 May 2008

establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005

Regulation EC 482/2008

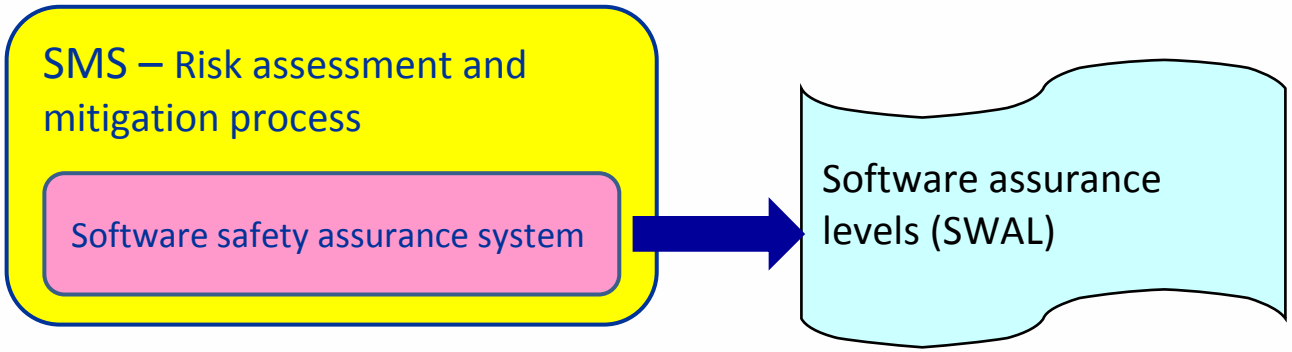
Article 4

Requirements applying to the software safety assurance system

The organisation shall ensure, as a minimum, that the software safety assurance system:

1.is documented, specifically as ***part of the overall risk assessment and mitigation*** documentation;

2. ***allocates software assurance levels*** to all operational EATMN software in compliance with the requirements set out in Annex I



Regulation EC 552/2004

Article 6
EC declaration of verification of systems

1. Systems shall be subject to an EC ***verification by the air navigation service provider*** in accordance with the relevant implementing rules for interoperability, in order to ***ensure that they meet the essential requirements*** of this Regulation and the implementing rules for interoperability, when integrated into the EATMN.

Essential requirement 3 - Safety

REGULATION (EC) No 552/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 March 2004

on the interoperability of the European Air Traffic Management network

(the interoperability Regulation)

Regulation EC 552/2004

Compliance:

- DoV for the “system” including:
  - DoC or DSU for constituents
  - Technical file with reference to evidence of compliance of ER and IR.

NSA

Gap – Quantitative safety levels

EU 1035/2011

3.1.2. Requirements for safety achievement
Within the operation of the SMS, providers of air traffic services shall:

(…)

(c) ensure that, wherever practicable, ***quantitative safety levels*** are derived and are maintained for all functional systems (quantitative safety levels);

FUNCTIONAL SYSTEMS

Gap - Functional system

What is a functional system?

‘functional system’ means a combination of systems, procedures and human resources organised to perform a function within the context of ATM

Annex I, par 3.2.1

b) the airborne, ground and, if appropriate, spatial components of the ATM functional system, through cooperation with responsible parties

Gap - Functional system

Systems (equipment)

Procedures

Human resources

Funcional System

$f(x)$

context of ATM

Airborne, ground and spatial components

Gap – Safety objectives

EU 1035/2011

'***safety objective***' means a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur;

(d) ensures that while providing air traffic services, the principal safety objective is to minimise its contribution to the risk of an aircraft accident as far as reasonably practicable (***safety objective***)

Safety objectives based on risk shall be established in terms of the hazard's maximum probability of occurrence, derived both from the severity of its effect, and from the maximum probability of the hazard's effect.

Gap – Hazards at service level

Existing hazards

Hazard ID	Function	Hazard	Operational Impact	Conditions	Severity Class	Justification / comments
II-TRK-1	Tracking	Undetected loss of tracks	Loss one or more tracks		2	**Note:** Usages of filters in the surveillance picture might cause this hazard; in case of mode C changes of assumed a/c. Also, a window might cover tracks. Flight Progress Strips, TTW and FPL track allow the detection of these losses. When there is high traffic load in the sector, the crosscheck with the Flight Progress Strips might not be performed in due time.

Corresponding Safety Objective

The probability of having an undetected loss one or more tracks in the Lisbon ACC shall not be higher than Rare.

Is this meaningful, measurable?
Is it worthwhile for the organization to keep track of all these events?

Implementation plan

- Define and establish safety levels
- Define the mapping of components for reg. 552
- Develop the Functional system description and architecture

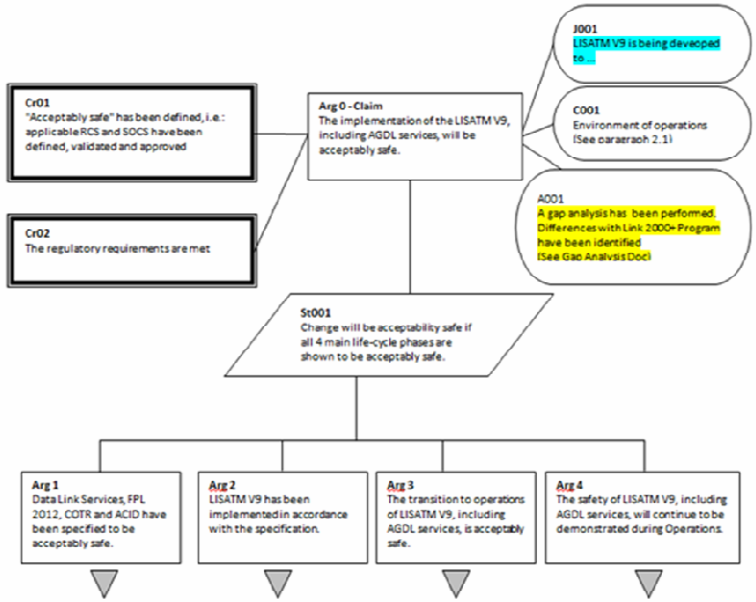
- Identify and evaluate barrier efficiency
- Determine safety objectives for constituents
- Define the safety requirements including SWAL

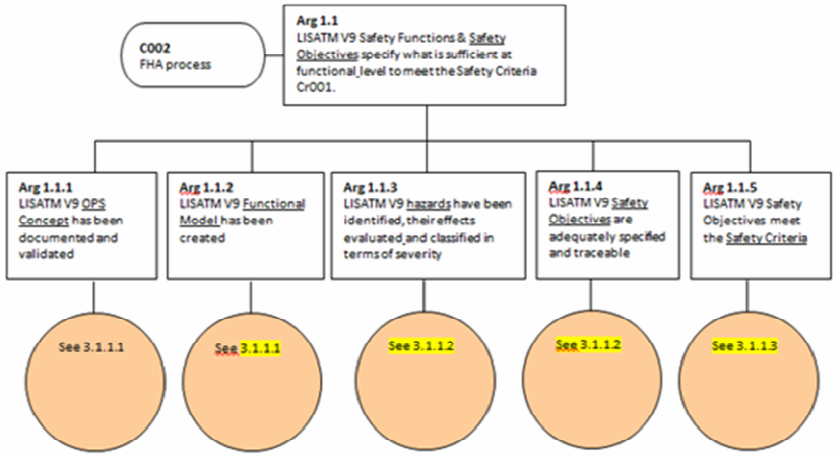
- Monitor fulfilment of safety objectives and safety requirements during the whole constituent lifecycle
- Ensure traceability of requirements until operations
- Build safety arguments for changes

Ensure the SMS covers these processes

Safety arguments for changes

Build safety arguments for changes





Safety arguments for changes

Also covers

•Produce Software Safety Assurance Manual

•Present generic compliance matrix for ED153 to NSA

The goal is to:

•Define requirements for implementing a SSAS in the SMS.

•Prepare a template for the software safety requirements to include in all call for tenders. **(Done and already in use)**

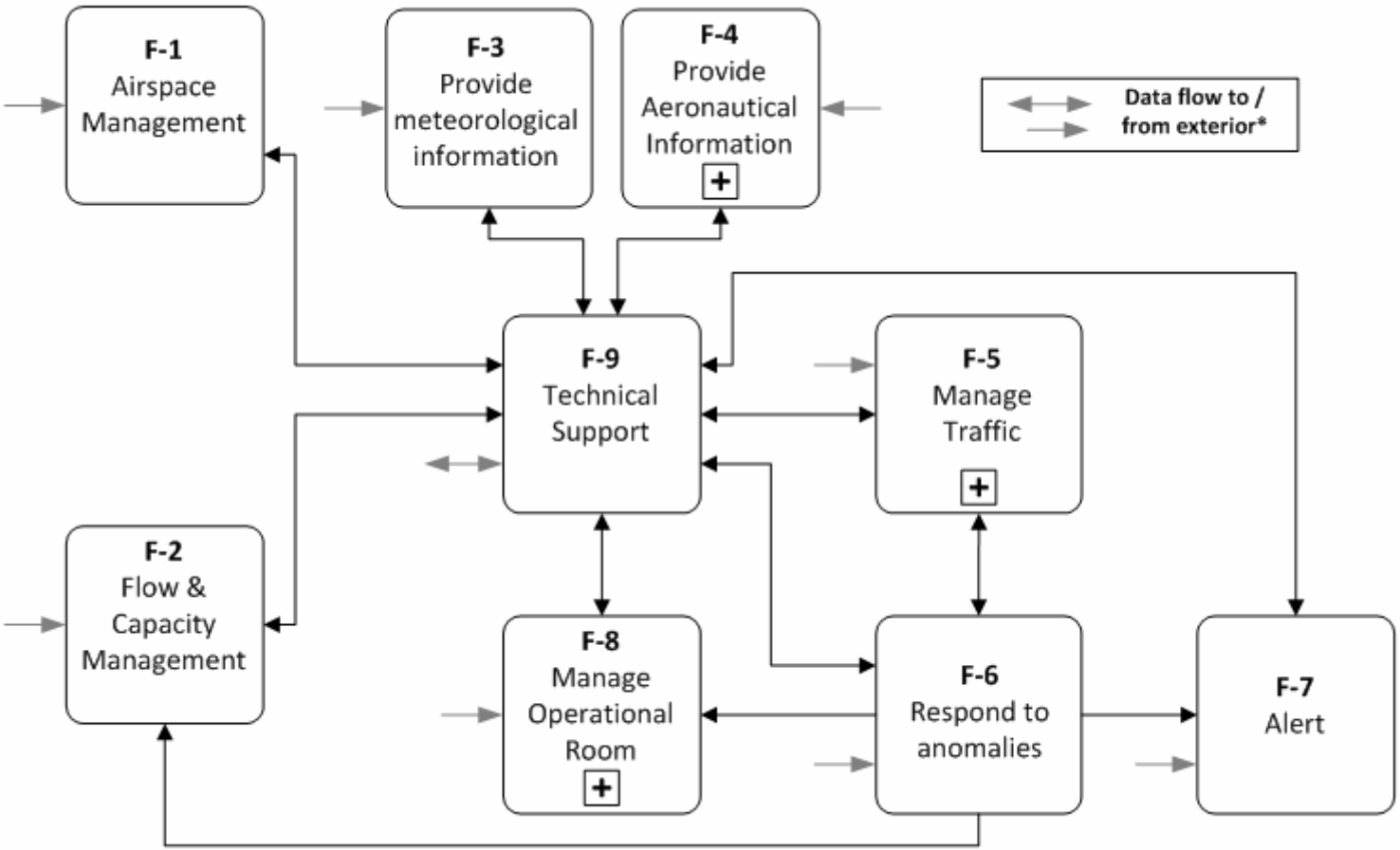
•Prepare a generic compliance matrix for regulation EC 482/2008, based on ED153 objectives. **(First revision on-going)**

This matrix will be the base for the projects software safety folder. Only the matrix cells with evidence coming from the project will have to be filled, all the others are pre-filled.

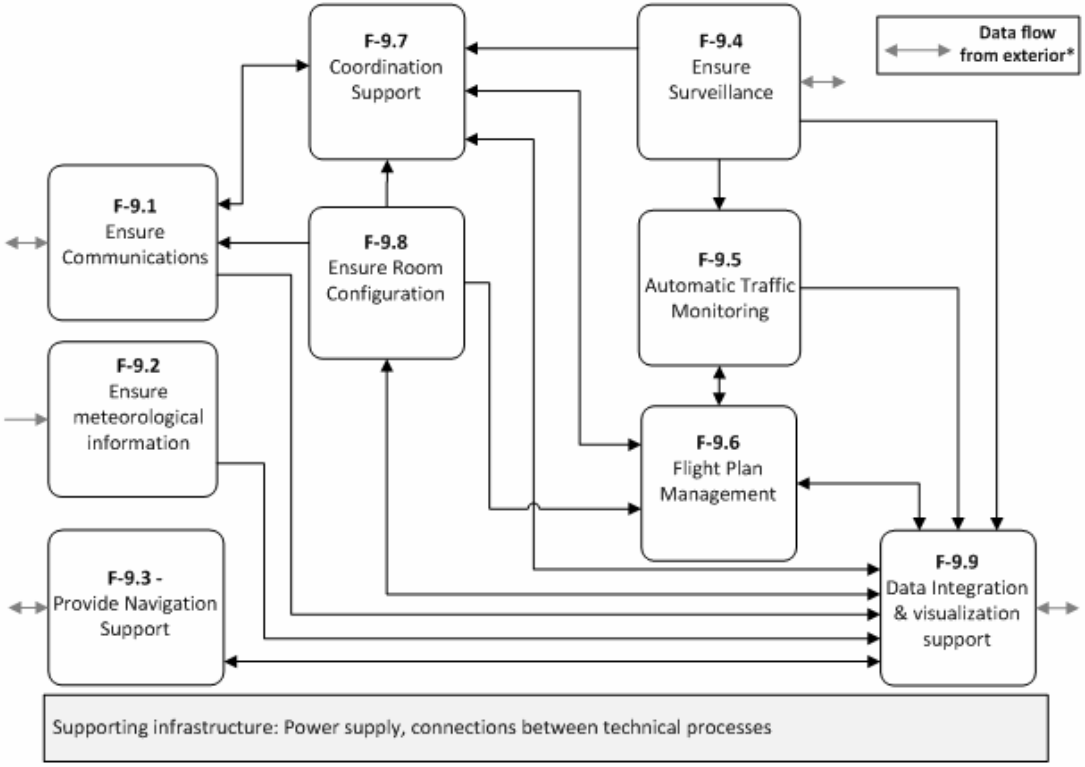
Achievements

Prepare and agree plan	Done
Task force management	On-going
WP1 – Concepts and System definition	
• Define and agree on concepts	Done
• Define safety levels	Done
• Develop functional system description	Done
• Develop functional system architecture	On-going
• Define EATMN representation of the systems (CATF)	Waiting
WP2 – Safety framing	
• Identify and evaluate barriers	On-going
• Determine safety objectives for constituents	On-going
• Define safety requirements definition including SWAL allocation	Waiting
WP3 - Operational Processes definition	
• Monitor safety objectives	
• Monitor safety requirements	
• Ensure traceability of safety requirements to operations	
• Build safety arguments for changes	
WP4 – SMS update	
• Update and review SMS	
• Support process application to specific cases	On-going

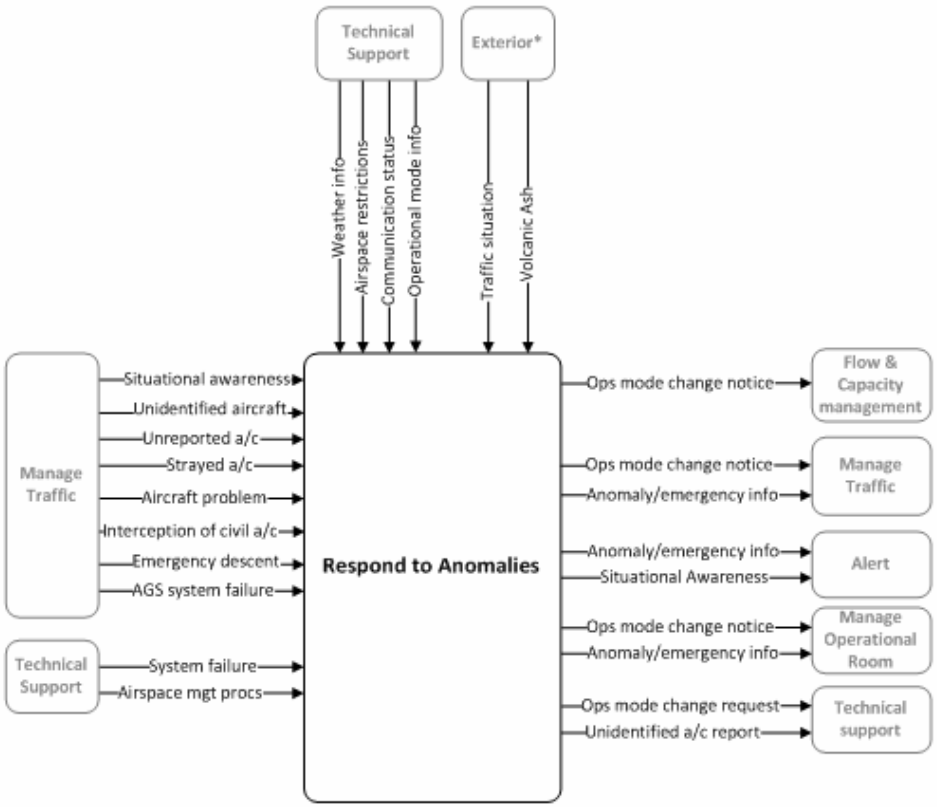
Functional System Description

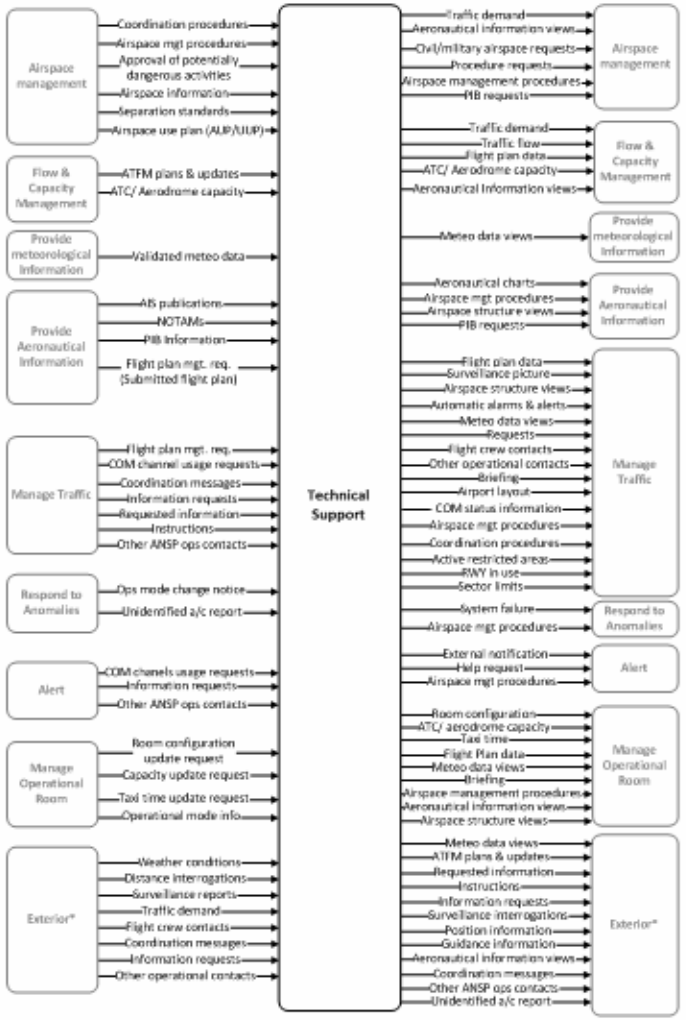


Functional System Description

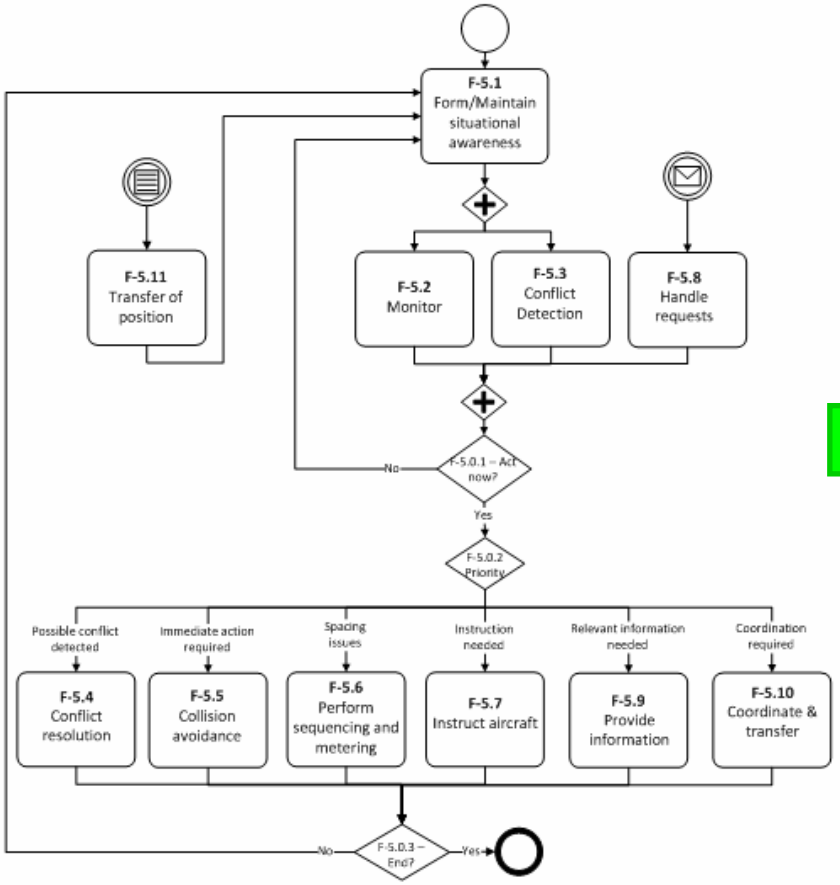


Functional System Description





Functional System Description



INAC
Instituto Nacional de Aviação Civil, I.P.

Functional System Description

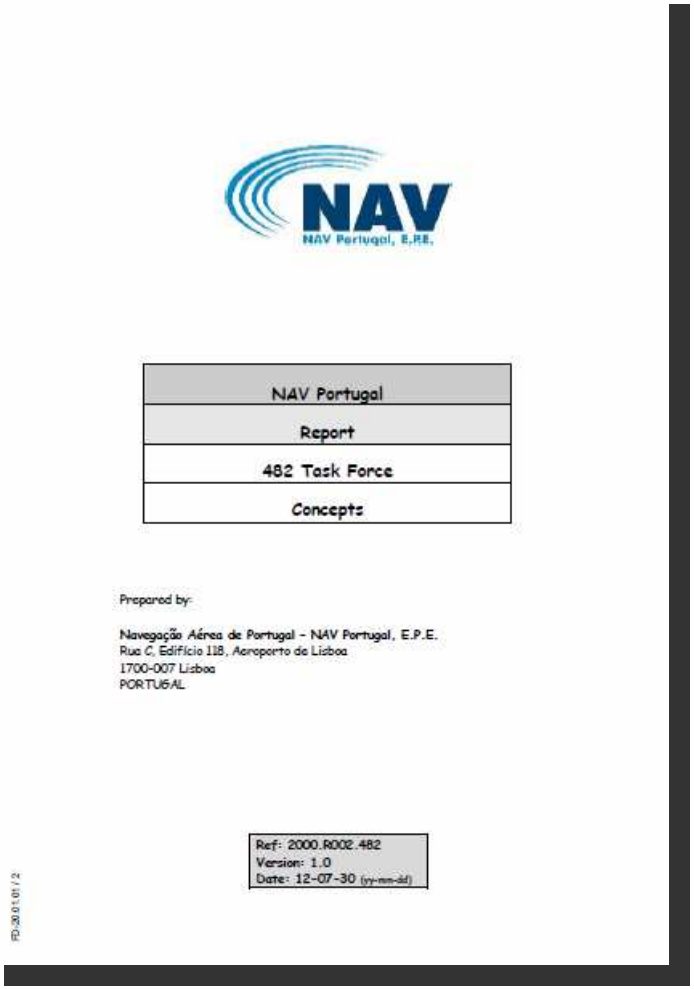
Technical system as centre of information exchange

Clear view of interfaces

Base for architecture definition

Mapped against AIM – OK.

Define & agree concepts



NAV Portugal

Report

482 Task Force

Concepts

Prepared by:

Navegação Aérea de Portugal – NAV Portugal, E.P.E.
Rua C, Edifício 118, Aeroporto de Lisboa
1700-007 Lisboa
PORTUGAL

Ref: 2000.R002.482
Version: 1.0
Date: 12-07-30 (yy-mm-dd)

Define & agree concepts

2.6 *Safety objective*

Regulation (EU) 1035/2011 (ref. [1]) and Regulation (CE) 482/2008 (ref. [3]) define:

'safety objective' means a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur;

A **safety objective** defines the maximum frequency or probability at which a hazard is accepted to occur.

Um objetivo de segurança define a frequência ou probabilidade máxima aceitável de ocorrência de uma situação de perigo.

INAC
Instituto Nacional de Aviação Civil, I.P.

Architecture

- Drills down on functional system description
- Includes enablers (implementation)
  - People (credentials)
  - Procedures
  - Equipment
- Automated generation due to complexity and to ensure coherence
- First draft reviewed, final version almost ready

Conclusions

- Without the risk assessment framework, it is not possible to comply with EC 482/2008

- Reg. EC 482/2008 has impact in the whole organization (design, purchases, maintenance, operations, …)

- Addressing software alone,

  is missing the point

No need to be perfect,
just good enough to start building on.

Questions