Certification & Oversight Of Air Navigation Service in EU system

Franck Giraud

Director of International Cooperation

Europe / CIS / Japan

DGAC

EIWACS 2013 – Tokyo

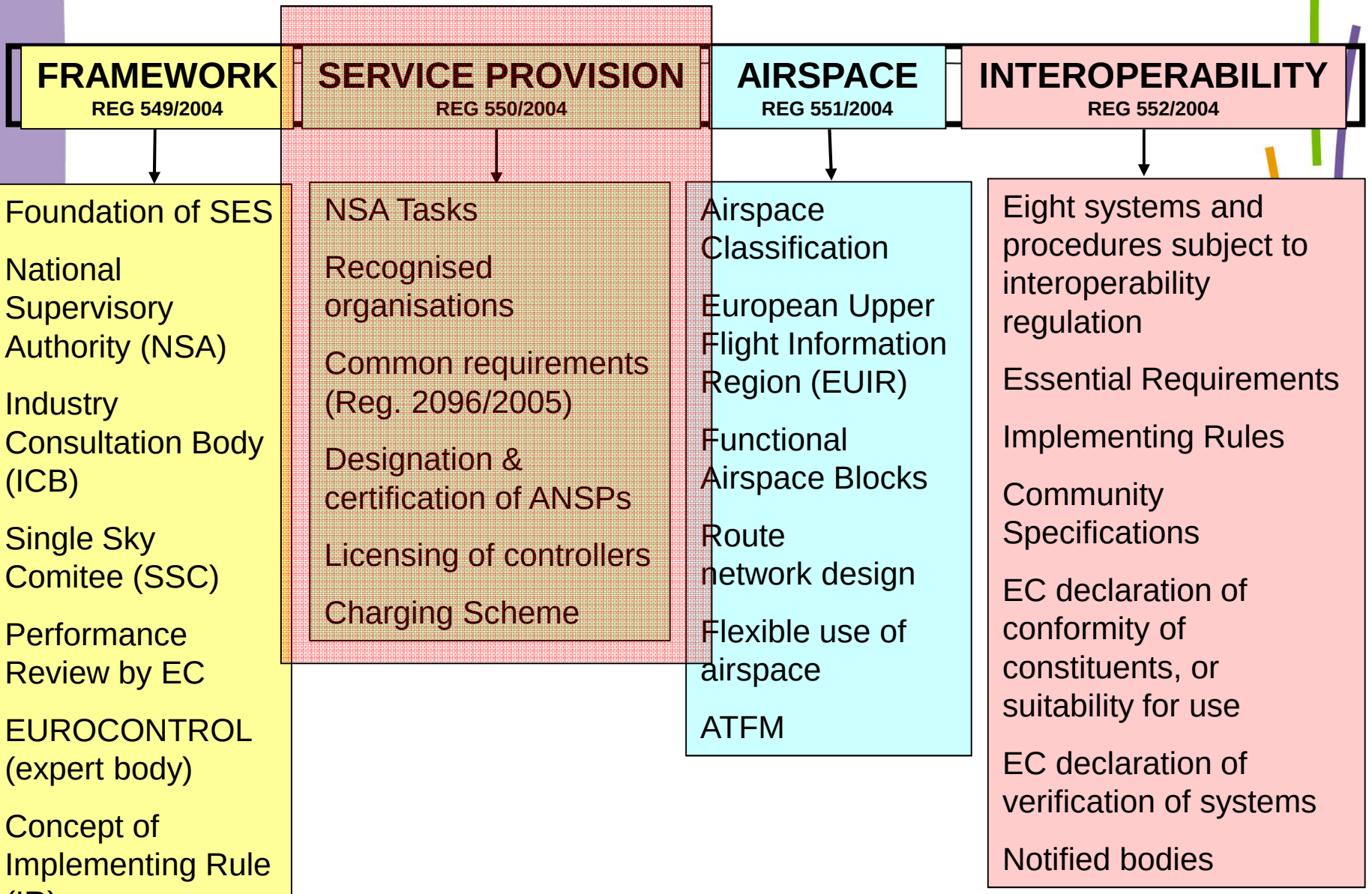
Summary

- **Context & History**
- **EU Principles of certification and surveillance in ANS**
  - **Certification of Air Navigation Service Providers (ANSPs)**
  - **Principles of continuous oversight**
  - **Application to technical systems**
    - **Safety cases**
    - **Software certification**
    - **Interoperability**
- **Conclusions**

Context & History

- **Before 1998 : No oversight of Air Navigation Services**
- **ANS Services were often in EU public entities (civil or military), auto regulated**
- **1998-2004: Europe decided to put in place the separation between provision of services and regulatory functions → Single European Sky I**
  - **Firstly, through EUCONTROL**
  - **Secondly, through European Commission**
- **2004 Onwards : States have to reorganize to implement those new requirements and associated processes**

Single European Sky I (SES I - 2004)



EU Principles of certification and surveillance in ANS

- **EC Regulation 550/2004, based on 3 concepts and activities:**

#1 - Certification of Air Navigation Service Providers

#2 - Continuous safety oversight

#3 – Specific applications to technical systems

- **Safety cases**
- **Software certification**
- **Interoperability**

#1 – Certification of ANSPs (1/2)

- **The Air Navigation Service Providers has to be certified by the National Supervisory Authorities**
- **The core of the certification requirements is based on Safety Management System (SMS)**
- **Some other general requirements are added such as:**
  - **Financial strength;**
  - **Insurance;**
  - **Organization structure;**
  - **…**

#1 – Certification of ANSPs (2/2)

- **Audit based process: the Authority checks every requirement before granting certificate:**
  - **All ATC Units have to be audited;**
  - **All requirements must be checked;**

- **SMS Principles:**
  - **Based on quality principles applied to safety;**
  - **Focus on:**
    - **Definition of responsibilities**
    - **Occurrence reporting in a non punitive environment**
    - **Safety analysis for any change in the system**
    - **Personnel competence (in general not only ATCOs or ATSEPs)**
    - **Internal safety audits**
    - **Management of external services**
    - **…**

#2 – Continuous Oversight

- **Once initial certification is done, a process of continuous oversight is put in place based on 3 layers:**
  - **Follow up of occurrence reports;**
  - **Approval of safety case when important changes occur to the system (new technical systems, new procedures)**
  - **Continuous management of competence (ATCO / ATSEP licences)**

- **The output of these activities shall drive the continuing audit programme**

  →Audit Management by the risk

#3 – Application to technical systems (1/7)

- **One issue to solve : what about the formal certification of technical systems?**
- **Should it be done for all existing systems?**
- **How can it be handled by brand new authorities?**
  - **Very technical;**
  - **Very often : no history;**
  - **Large number of existing systems;**

#3 – Application to technical systems(2/7)

Two principles :

1. No certification of existing systems:

- **Exsiting system are considered as « safe »**
- **Impossible to make a certification from scratch on existing systems**

2. No certification as such for technical systems

#3 – Application to technical systems(3/7)

3 ways of making the supervision on technical systems:

#1 – Guarantee the safety of changes

#2 – Apply specific regulation on operationnal software

#3 – Apply specific requirements for interoperability of systems all around europe.

#3 – Application to technical systems (4/7)

#1 – Guarantee the safety of changes

- **Each time an ATM system has to be changed or updated:**
  - **The provider makes a safety analysis**
  - **This analysis shall aim at identifying the safety criticality of the change**
  - **This safety analysis is approved (for critical changes) by the Authority**

#3 – Application to technical systems (5/7)

#2 – Apply specific regulation on operational software (*Regulation (EC) n° 482/2008)*

- **ANSP shall demonstrate (argument and evidence) that requirements below are satisfied:**
  - **Software safety requirements validity**
  - **Software verification**
  - **Software configuration management**
  - **Software requirements traceability**
  - **No functions which adversely affect safety**
- **ANSP shall allocate software safety assurance levels which is consistent with the criticality of the software (from 1 to 5)**

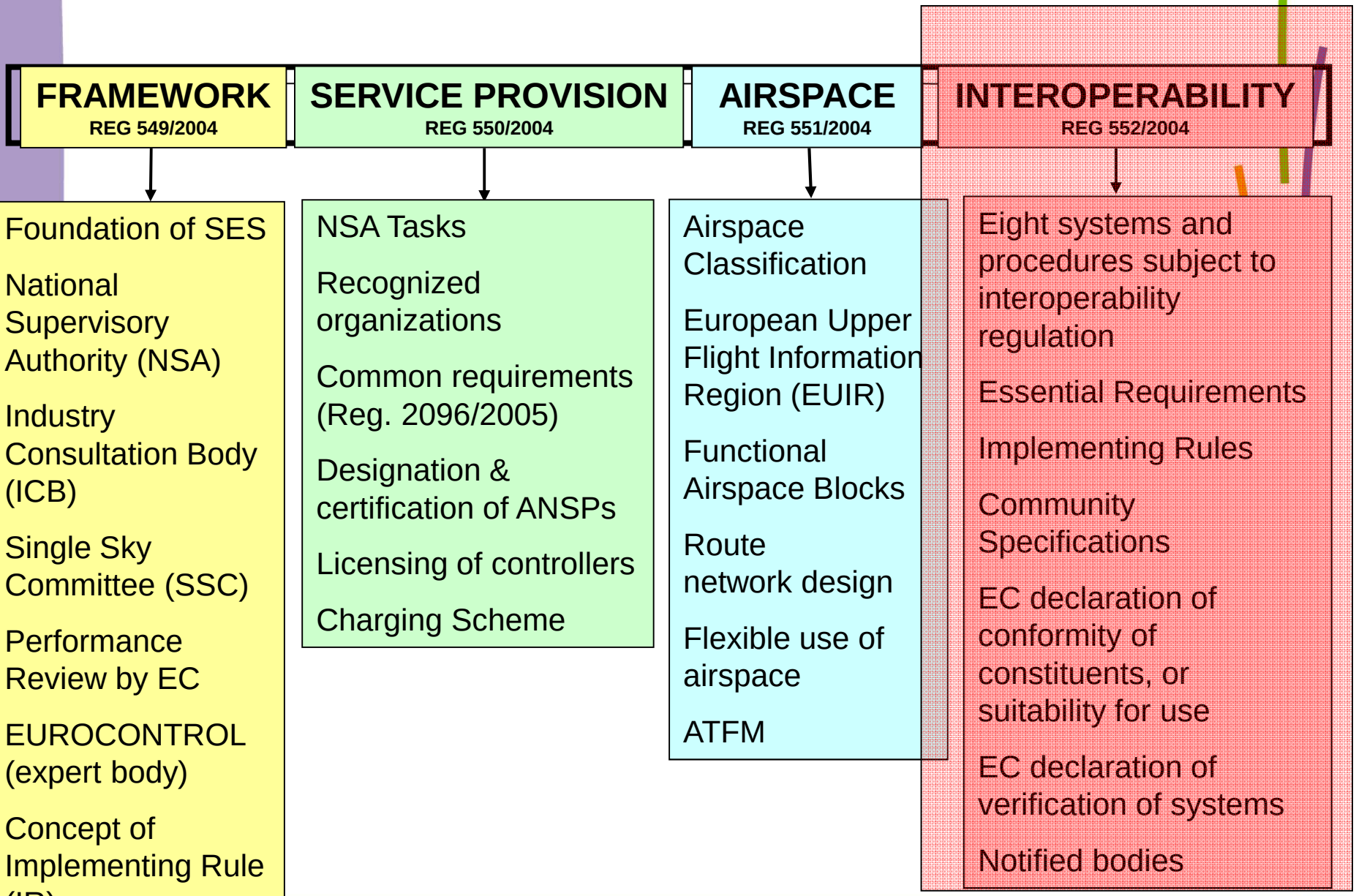
#3 – Application to technical systems (6/7)

#3 – Apply specific requirements for interoperability of systems all around Europe

- **In order to be interoperable, the technical systems have to meet common EC technical requirements**

- **Those requirements are contained in EC regulations, and are still being developed.**

Single European Sky I (SES I - 2004)



15

#3 – Application to technical systems (7/7)

Some of the regulation already published (non-exhaustive) :

- ***No 1033/2006 : Procedures for flight plans in the pre-flight phase***
- ***No 1032/2006 : Automatic systems for the exchange of flight data for the purpose of notification, coordination and transfer of flights between air traffic control units***
- ***No 633/2007 : Flight message transfer protocol used for the purpose of notification, coordination and transfer of flights between air traffic control units***
- ***No 1265/2007 : Air ground voice channel spacing***
- ***No 29/2009 : Data link services***
- ***No 30/2009 : Automatic systems for the exchange of flight data***
- ***No 677/2011 : Implementation of air traffic management (ATM) network functions***
- ***…***

Conclusions

- **Oversight by the authority based on audits**
- **Requirements for the ANSP mostly based on Safety Management Systems (SMS)**
- **Continuous oversight after certification**
- **No certification of technical systems by the authority as such but :**
  - **Approvals by the authority for critical changes;**
  - **Software specific regulation;**
  - **Interoperability regulations.**

Questions ?