Assessment of changes to functional systems in ATM/ANS and the oversight thereof

Entry Point North Seminar: The changing landscape of ATM Safety
Malmo, 26th -27th May 2015

Jose L Garcia-Chico Gomez
ATM/ANS Regulations Officer
FS4.2 ATM/ANS section
jose-luis.garcia-chico@easa.europa.eu

Flight Standards Directorate, EASA

Your safety is our mission.

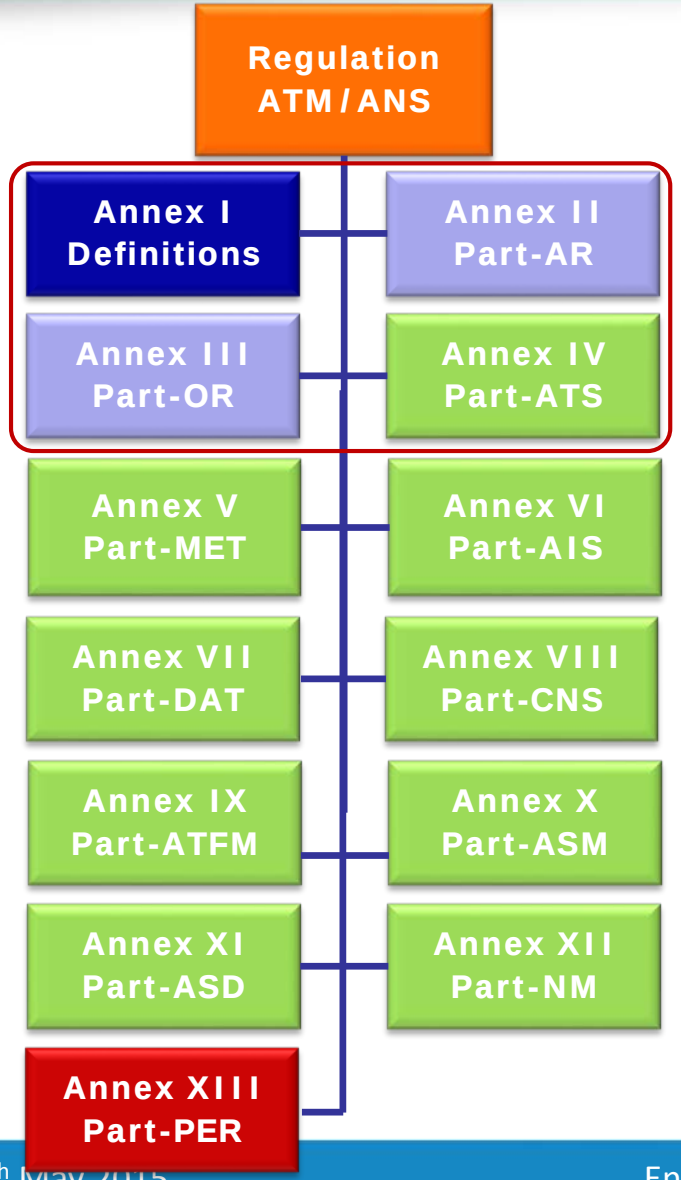
An agency of the European Union

- Background
- Functional system
- Underpinning Principles
- Safety & Safety Support Assurance
- Multiactor changes
- Proxies

What the new regulation introduces…

- **Evolution** from current regulations EU 1034/2011 and 1035/2011
  - Less process-based
  - support and extend current practices
  - Reduce subjectivity
  - Add flexibility: alternatives to risk assessment
  - not all service providers to perform safety assessments

Where in the future ATM/ANS rule structure? Provisions distributed in several Aneexes



General requirements

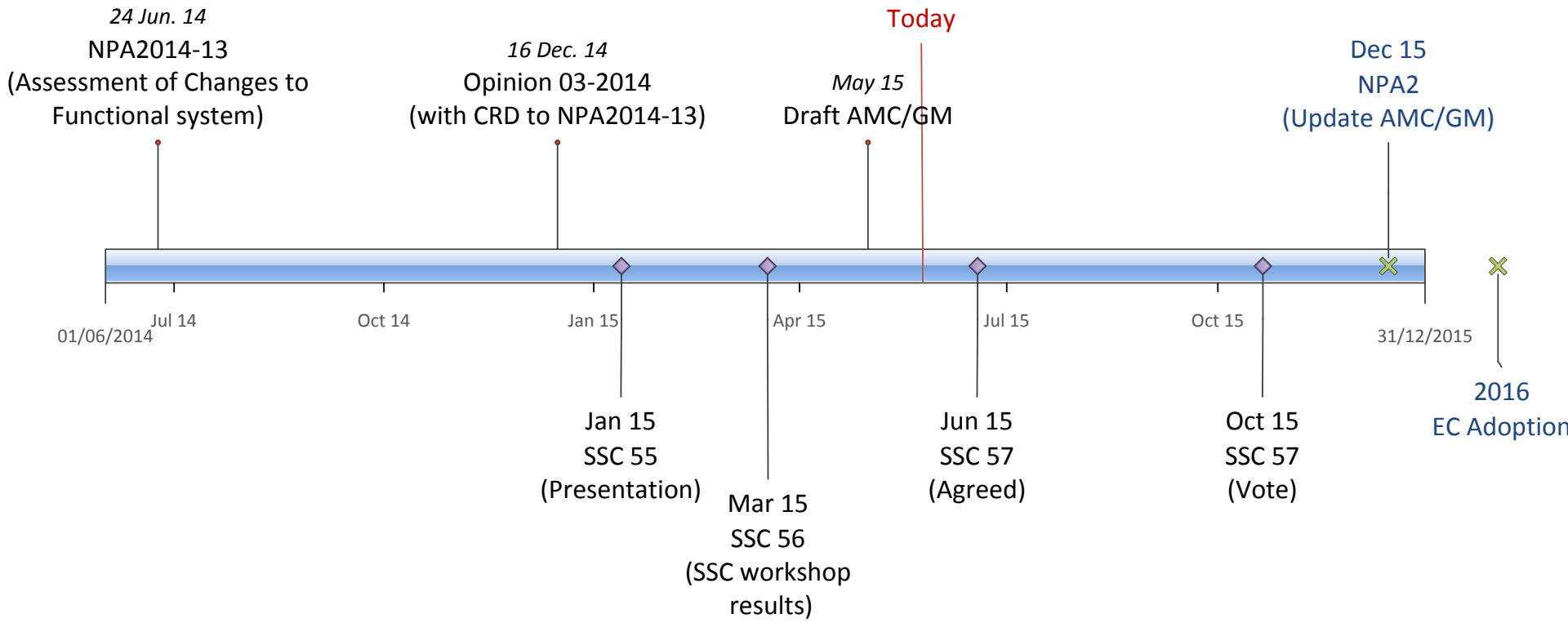
- **Part-AR:** Authority requirements
- **Part-OR:** Organisation requirements

Specific service requirements

- **Part-ATS:** Air Traffic Services
- **Part-MET**: Meteorological services
- **Part-AIS:** Aeronautical Information Services
- **Part-DAT:** Data providers
- **Part-CNS:** Communication, Navigation, Surveillance
- **Part-ATFM:** Air Traffic Flow Management
- **Part-ASM:** Airspace Management
- **Part-ASD:** Airspace Design
- **Part-NM:** Network Manager

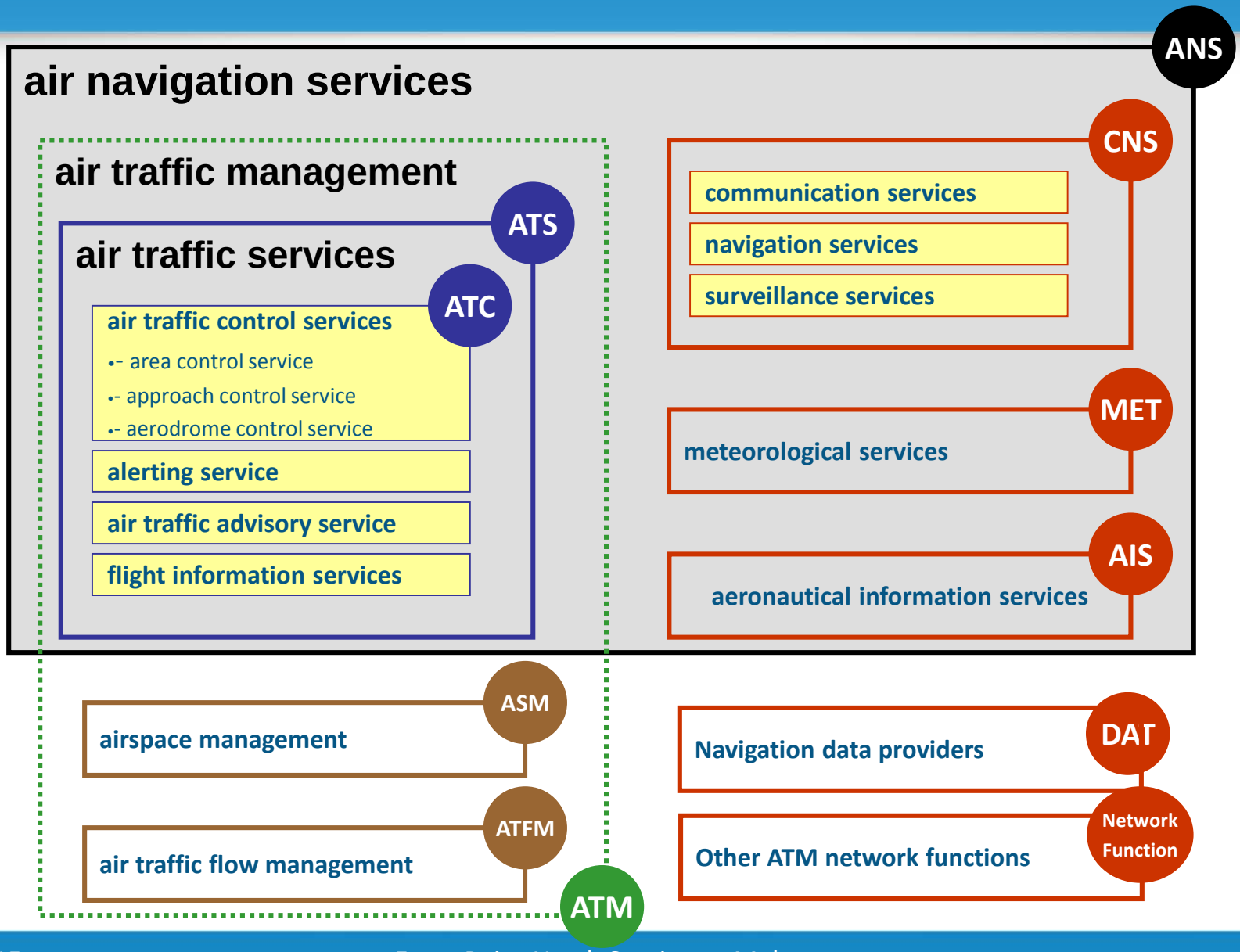
- **Part-PER:** Personnel requirements

Timeline for ‘assessment of changes’



- Background
- **Functional system**
- Underpinning Principles
- Safety & Safety Support Assurance
- Multiactor changes
- Proxies

Scope: what services are addressed?



Planned changes to functional system

- What is a functional system?

A combination of equipment (SW and HW), procedures and human resources organised to perform a function within the context of ATM/ANS and other ATM network functions

Two types of changes

- Unplanned change*: due to people adapting their behaviour to suit the operational circumstances e.g.:
  - seeking improvements - self motivated
  - changing their goals/motives,
  - adapting to unforeseen circumstances:
    - wrongly designed technical systems or services
    - changes in the operational context

- Planned change: Somebody notices that a change is needed and gets permission for the organisation to make a change

(*) These should be identified by monitoring the functional system and corrected where necessary…through planned changes

Examples of changes

- Examples:
  - Airspace changes-reorganisation;
  - Changed or introduction of communication, navigation, or surveillance system;
  - Changes or new approach procedure;
  - Introduction of automation to replace/assist human actions;
  - New automatic meteorological information;
  - Introduction of time-based separation;
  - Etc…

- Background
- Functional system
- **Underpinning Principles**
- Safety & Safety Support Assurance
- Multiactor changes
- Proxies

Principles: ATM/ANS providers (I)

- The ATM/ANS provider should be aware when a change to the operational (functional) system is necessary and it should make the change in a timely manner *(Change Drivers – proactive change)*
- No change should be made unless it can be shown that the ATS will be acceptably safe, via a valid assurance case, prior to its implementation.
- The CA is notified of the intention to make a change. Notification should give the CA sufficient time to review it.
- Where a CA review is to be performed, it has to be approved by the CA, before implementation. *(Notification involved – simpler for routine changes)*
- Even if the CA doesn't review the change the provider must ensure that a valid assurance case exists before the change is implemented.

Principles: ATM/ANS providers (II)

- Changes by ATS providers require safety assessment and assurance to show they are acceptably safe. Changes by other service providers require safety support assessment and assurance to show they are acceptably trustworthy *(safety assurance/safety support assurance)*

- Changes often involve change by many independent stakeholders, these should be managed as though they were a single change *(Coordination of multi-actor changes)*

- The provider must monitor the behaviour of the system using monitoring criteria included in the assurance case and, where necessary, introduce new changes. *(Change Drivers – monitoring)*

Principles: ATM/ANS providers (III)

- The acceptable level of safety for the change must be decided and declared by the service provider in terms of safety risk or other measures related to safety risks.

  (Proxies, recognised standards/practices)

- Safety criteria should be based on the notion that the operational (functional) system should
  - support the improvement of safety whenever reasonably practicable;
  - be at least as safe after the change as it was before; or
  - the loss on safety is
    - Temporal: to be offset in the future
    - Permanent: other beneficial consequences

  (Objective for safety)

Principles: competent authorities

- The CA, when notified of the intention to make a change, seeks the data on which the decision, whether to review the change or not, will be based

- The CA decides whether to review the change or not
  - The decision should use objective risk based criteria *(Risk posed by the change)*
  - The rigour of the review (its breadth and depth) should be proportional to risk *(Risk associated with the change)*.*

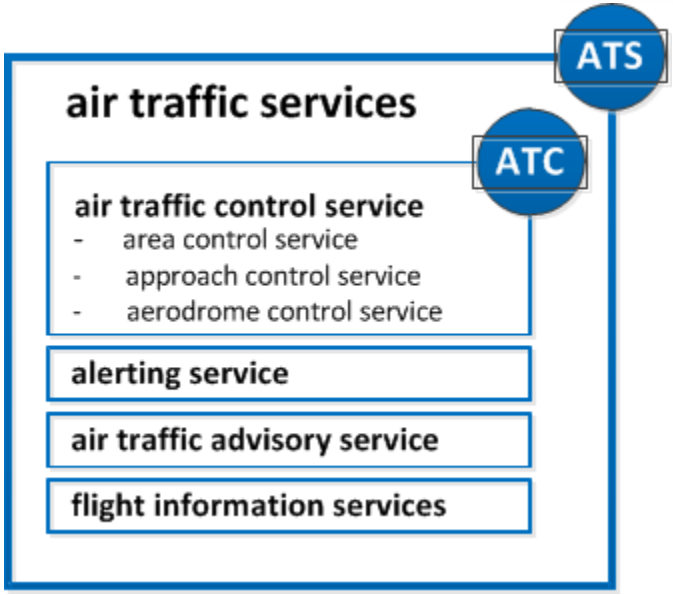
- Changes involving several providers may also involve several CAs. These CAs need to cooperate in reviewing the change *(multi-actor change)*

(*) Not present in the rule at the moment.

- Background
- Functional system
- Underpinning Principles
- **Safety & Safety Support Assurance**
- Multiactor changes
- Proxies

The view of safety* - 1

- ATS providers can:
  - communicate with Aircraft
  - provide traffic information
  - understand the intent of traffic
  - provide separation

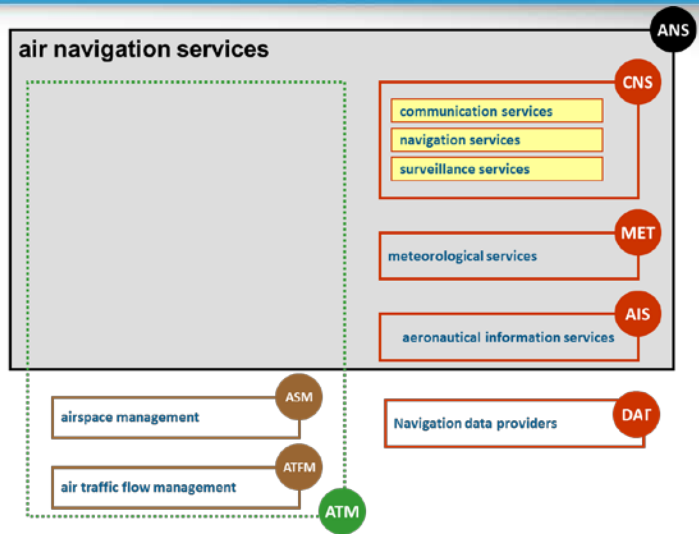


- They:
  - can **intervene** if they **see** an unsafe situation developing
  - have **a "view" of safety**

**Safety related to aircraft separation*

The view of safety - 2

- ATM/ANS providers other than ATS providers are unable to:
  - communicate with Aircraft
  - provide traffic information
  - understand the intent of traffic
  - provide separation
- They
  - only have partial knowledge
  - can not **intervene** when an unsafe situation develops
  - do not have **a "view" of safety**

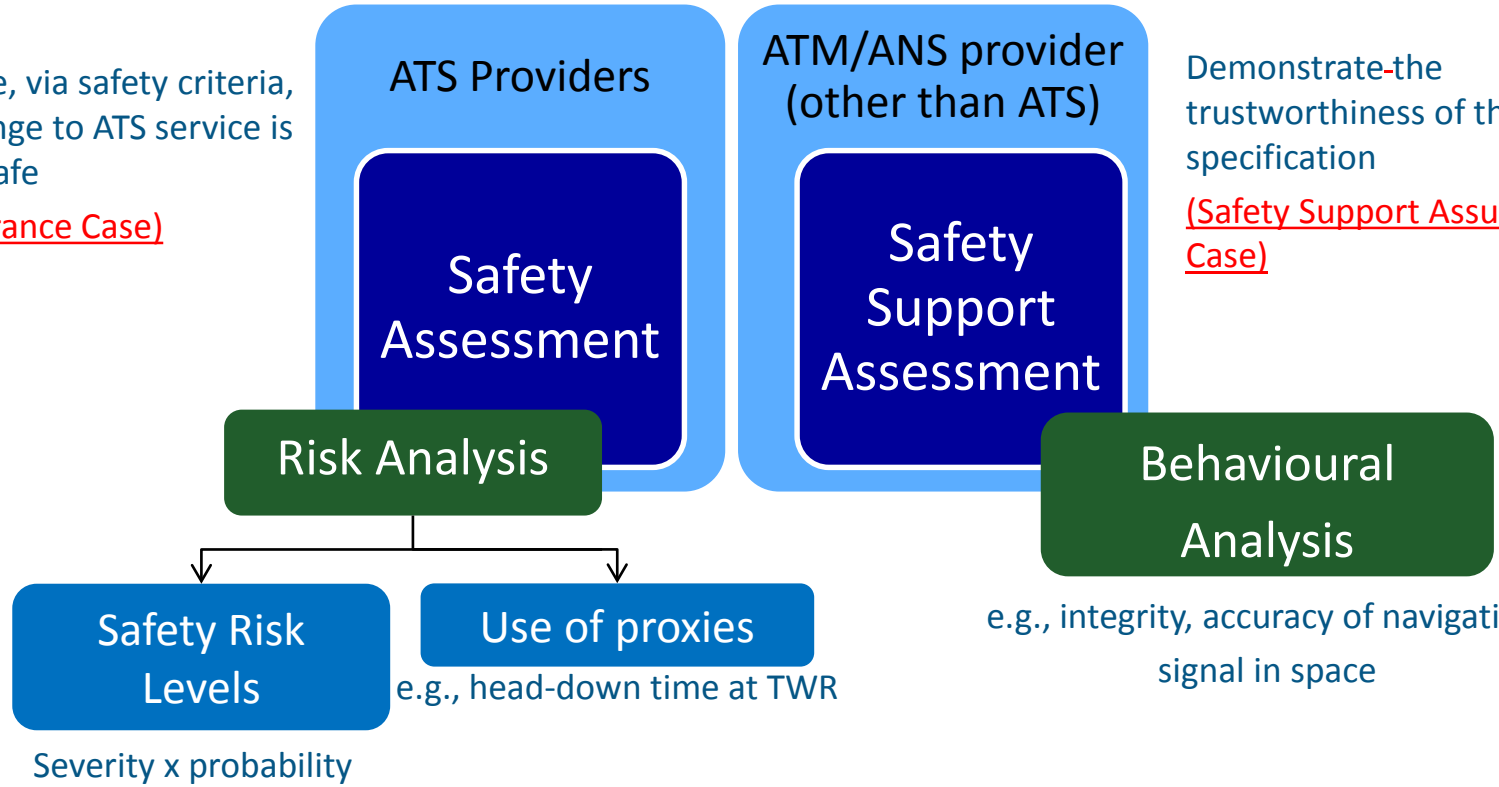


Safety assessment & Safety support assessment: The need and the focus

- All service providers need to assess changes they make to their functional system, but…

demonstrate, via safety criteria, that the change to ATS service is acceptable safe

(Safety Assurance Case)



Severity x probability

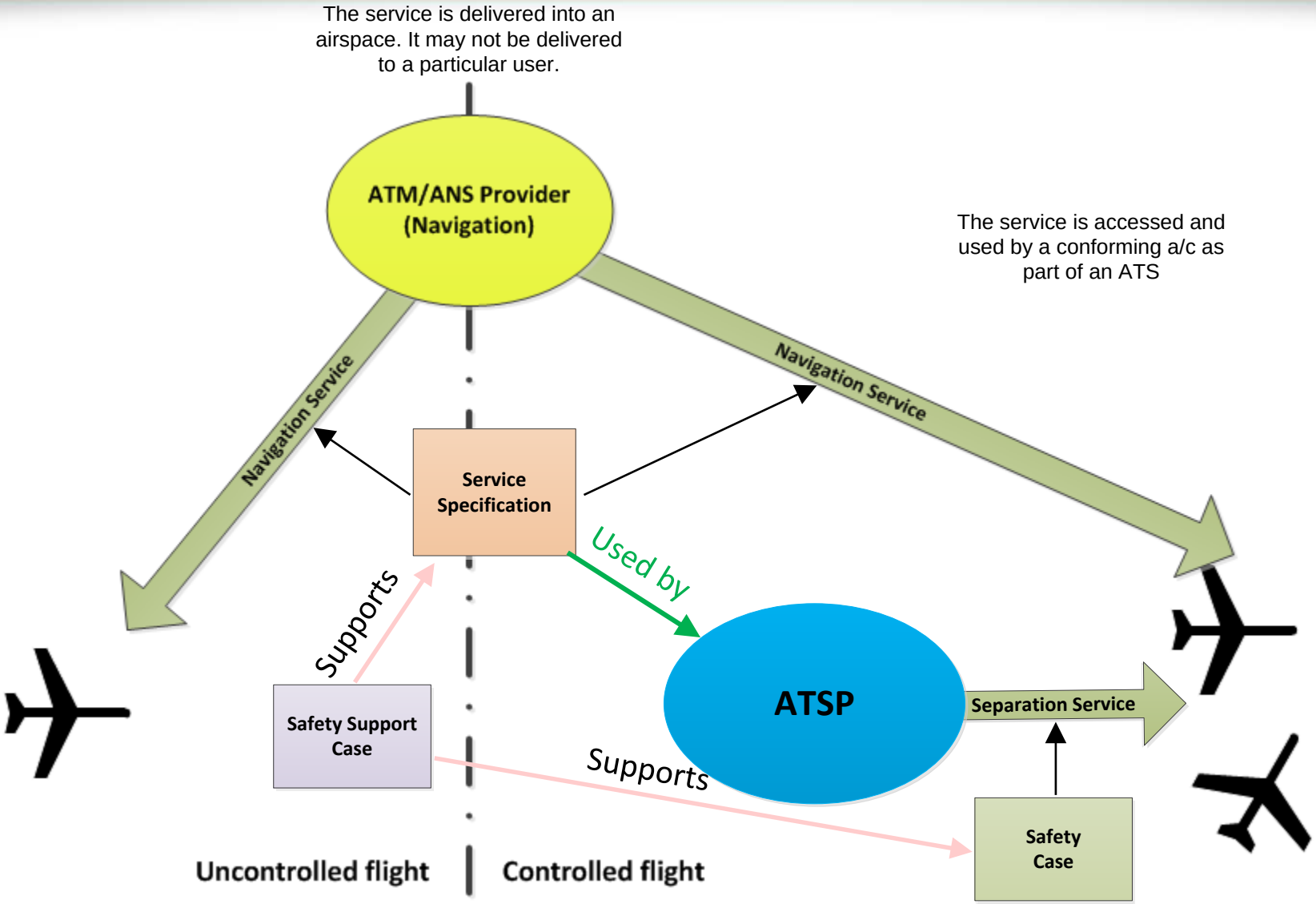
e.g., head-down time at TWR

Demonstrate the trustworthiness of the specification

(Safety Support Assurance Case)

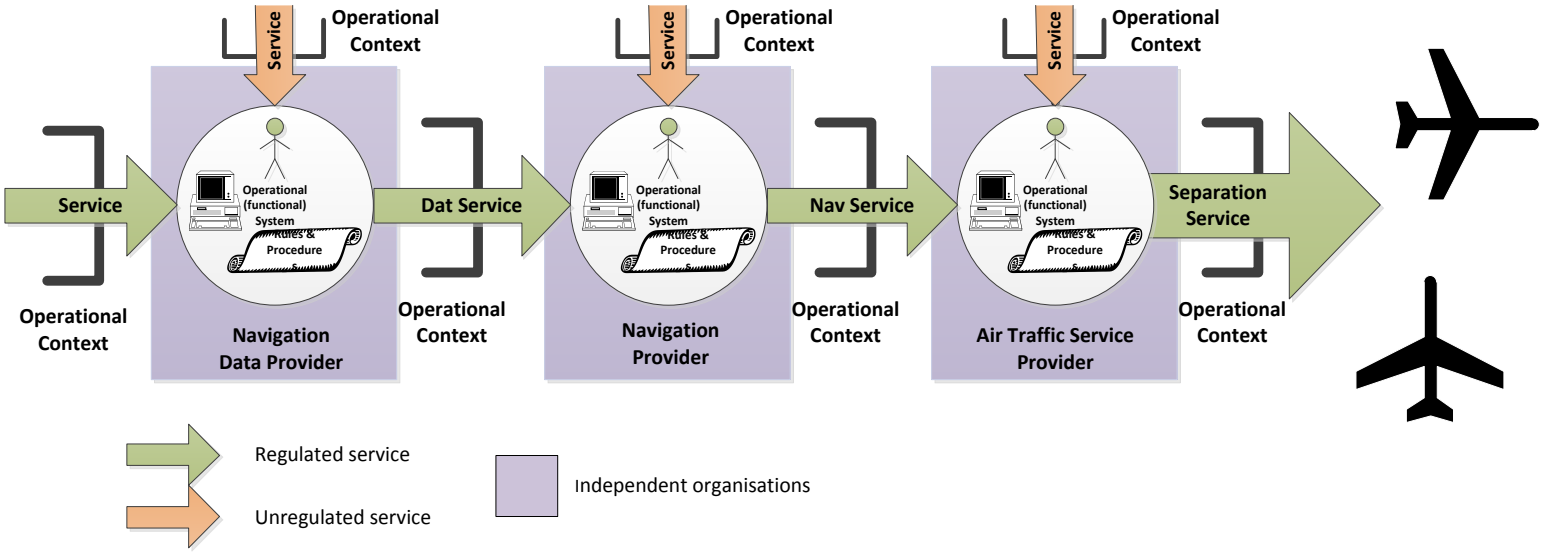
e.g., integrity, accuracy of navigation signal in space

Safety Assurance & Safety Support Assurance: an example of interaction

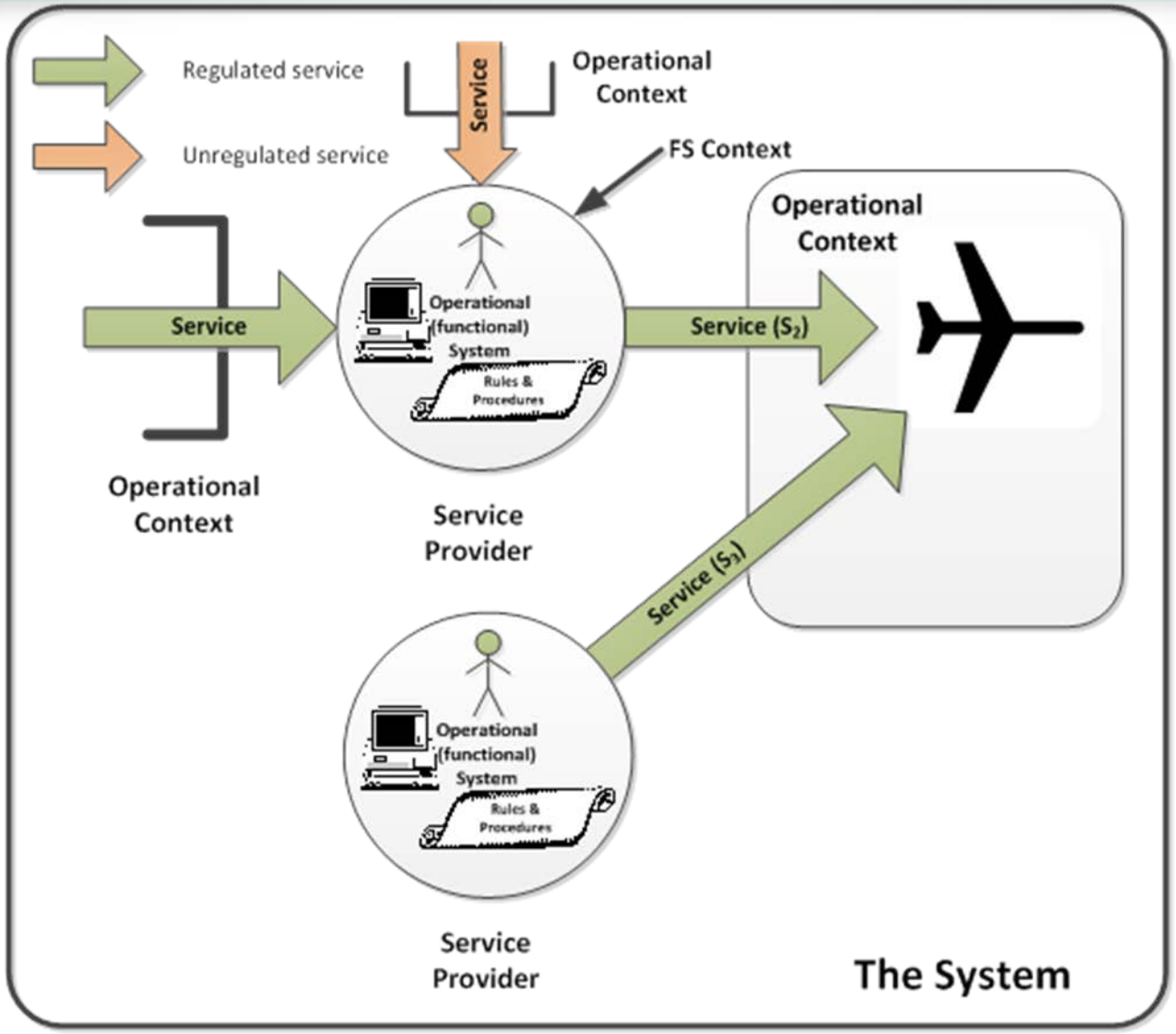


- Background
- Functional system
- Underpinning Principles
- Safety & Safety Support Assurance
- **Multiactor changes**
- Proxies

Multiactor changes (notion) 1



Multiactor changes (notion) 2



Description seems straight forward, but is it really?

Any change to the functional system of an ATM/ANS provider affecting other ATM/ANS providers and/or aviation undertakings

The need for specific provisions dealing with changes affecting multiple actors is real

- Account for cascade effects of changes to third parties…and feedback effects
  - ATM system is a complex and interconnected system
  - Multiple interdependencies

- Different “view” of safety of ATM/ANS providers

When a change affects other stakeholders: dependencies & interdependencies

- A change may modify:
  - Service (e.g., reduction of separation)
  - Operational environment (e.g., airspace structure)

- Other ATM/ANS or aviation undertaking may be affected:
  - (as end user)
    - Use the affected service
    - Operate in the affected environment
  - (if they deliver service to others)
    - Deliver a service making use of the affected service
    - Deliver a service in the affected environment

The ATM/ANS provider proposing a change affecting multiple actors…

1. **Notify** all affected stakeholders to the CA

2. **Coordinate** activities with other affected ATM/ANS providers to:
   a. Identify all dependencies
   b. Identify assumptions and mitigations that relate to multiple actors

3. Use only **aligned and agreed** assumptions and common mitigations

   or alternatively:

   a. use an additional body of evidence,
   b. engage a representative body of av. undertakings,

Competent authorities coordinating in MAC

- Only when the service providers are not under the oversight of a single CA

  ① Use the process to establish **coordination arrangements** with other CAs

  ② Ultimate aim is to ensure effective **selection and review** of related changes

- CAs will decide the best way to ensure it
- Within FABs, suitable coordination may be based on current FAB arrangements

- Background
- Functional system
- **Underpinning Principles**
- **Safety & Safety Support Assurance**
- Multiactor changes
- **Proxies**

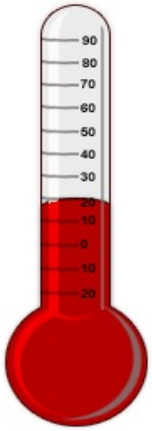
Flexibility introduced about “HOW”

- **Safety criteria**: specific and verifiable criteria used for the safety acceptability of a change
  - explicit quantitative acceptable safety risk levels; or
  - Proxies; or
  - recognised standards and/or codes of practice; or
  - the safety performance of the existing system or a similar system elsewhere

Proxies used as a surrogate of safety risk

PROXY:

A measurable property that relates to safety risk, but is more accessible than safety risk



1. Justifiable casual relationship exists between the proxy and the safety risk
2. Sufficiently isolated from other proxies
3. Measurable to an adequate degree of certainty

Examples of proxies:

head-down time, workload , error rate, false alert rates, service continuity

Why the use proxies?

- to facilitate the focus on the analysis and mitigations of the identified hazards: positive effects of changes
- to save resources when extra effort to identify, describe, and analyse the complete sequence of events from hazards to accidents has no added value
- to compensate for the lack of evidence on the probability of some events
- to facilitate the recognition of safety issues by operational staff
  - Facilitating communication and buy-in of changes

- Evolution of current rules (less process-based)
- Safety assessment vs Safety support assessment
- Multiactor changes
- Alternatives to use explicit risk metric

EASA
European Aviation Safety Agency

Questions?