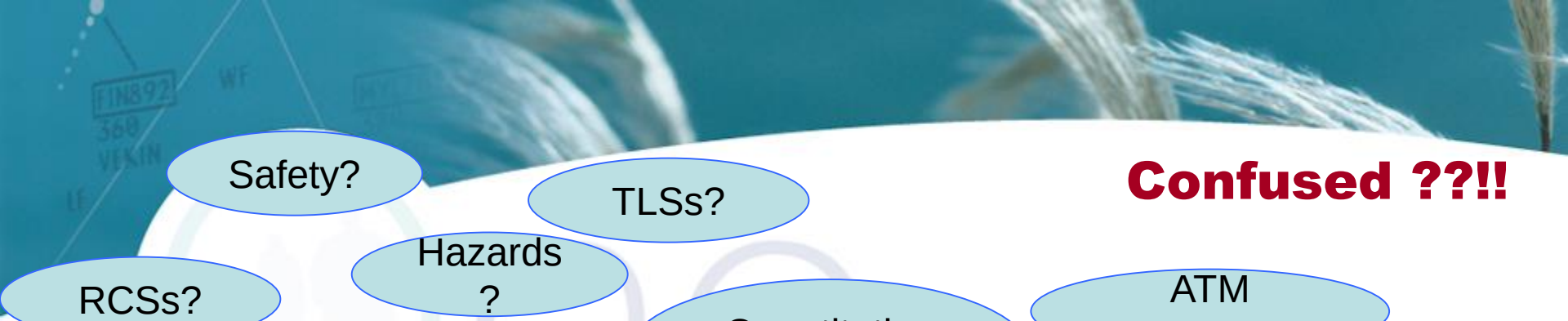
Safety Assessment Training Workshop

Safety Assessment – Concepts and FAQs

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL



Safety?

TLSs?

Hazards ?

RCSs?

Quantitative or Qualitative?

ATM 2000+?

Relative or Absolute?

ESARR 4?

ATM “direct contribution” ?

Safety Assurance?

Safety Cases?

Safety Plans?

SCDM?

SAM ?

Safety Requirements?

SWALs?

ESARR 3?

HF Case?

PALs?

Simulations?

SMS?

HALs?

HRA?

Unit Safety Cases?

ESARR 2?

CTA?

IRP ?

Safety Screening?

Success Approach?

SES ?

Safety Monitoring?

Confused ??!!

What is 'Safety'?

- Defined in ESARR 4 as 'freedom from unacceptable harm'.
- *Harm* is understood to mean an accident involving death / serious injury to personnel and/or major structural damage to aircraft.

A *safe* situation exists when the risk of an accident is *acceptably* low – see next slide

EUROCONTROL

How Safe do we need to be?

- ATM 2000+ requires the risk of an accident not to increase [with time] and preferably decrease
- ESARR 4 provides a quantification of ATM 2000+, for design of new systems / changes to existing systems:
  - maximum [tolerable] risk of an accident of 1.55x10-8 per flight hour
  - applies to overall ATM service, not to specific changes
  - takes account of the predicted increase in traffic up to the year 2015
- ESARR 3 places obligation on ANSPs to ”reduce risk as far as reasonably practicable” [*AFARP*]
- the SES Mandate given to EUROCONTROL to develop a [tolerable] Risk Classification Scheme
  - will require setting of ECAC-wide and national Safety Targets for ATM design

In general, acceptable = tolerable + AFARP

How do we show how Safe we are?

- By carrying out a Safety Assessment comprising typically:
  - an **a priori** *risk assessment and mitigation* of changes to the ATM system, in compliance with ESARR 4 and SES CR 2096/2005
  - **in-service** *safety monitoring* of on-going operations, in compliance with ESARR 2 and EC directive XXX
  - **in-service** *incident investigation and corrective action*, in relation to on-going operations, accordance with ESARR 2 and EC directive XXX – this is a very important contributor to the achievement of the *AFARP* objective
  - **in-service** *safety surveys* of on-going operations in compliance with ESARR 3 and SES CR 2096/2005

EUROCONTROL

Risk Assessments – historical perspective

- Derived from SAE ARP 4754 / 4761 (civil airborne systems):
  - Equipment focused
  - Failure based:
    - Safety Requirements mainly about reliability
- Maybe not a major problem historically for ATM because:
  - Systems have not been highly integrated
  - Changes have been largely equipment replacement
  - Operational changes have been evolutionary

But it is a problem for the future – new concepts, automation etc

A broader approach to *a priori* Risk Assessment and Mitigation

- ***Success*** approach:
  - to show that an ATM system will be acceptably safe in the **absence** of failure
  - addresses the ATM contribution to aviation **safety**
  - defined by Functional Safety Requirements
- ***Failure*** approach:
  - to show that an ATM system will still be is acceptably safe, taking account of the possibility of (infrequent) failure
  - addresses the ATM contribution to aviation **risk**
  - defined by Safety Integrity Requirements

Much more detail on this in the next Session!!

EUROCONTROL

Mini Exercise – a very simple example

- What properties make a car airbag safe??
- Show which properties apply to:
  - Preventing injury
  - Causing injury (hint: omission and commission!)
- Complete the following statement: “The airbag in <<this car>> is safe because….”:
  1. ?
  2. ?

Airbag Exercise – Debrief (1)

- Injury-prevention properties:
  - size; shape; inflated volume; location; material strength; compressibility; sensitivity of deployment mechanism; speed of deployment; etc
- Injury–causation properties:
  - reliability (probability that it will deploy when required)
  - integrity / sensitivity of deployment mechanism (probability that it will not deploy when not required)

- 1st set are determined by the requirement to reduce pre-existing risk in the *system's* operational environment
- 2nd set are determined by the need to limit any increase in risk due to failure of the *system*

This leads us on to ……

Airbag Exercise – Debrief (2)

"The airbag in <<this car>> is safe because….":

1. In the event of a head-on collision, it makes a major contribution to the reduction in the risk of death / serious injury, when working to specification
2. Any increase in the risk of death / serious injury due to failure to operate when required, or spurious operation when not required, is small compared with the safety benefit

- The lead-in statement is a (top-level) safety *Claim*
- If we can show that the two supporting statements are true, then we can say that the Claim is true
- We need evidence to show that the two supporting statements are true
- Then we have a Safety Case!!

The two supporting statements are known as *Safety Arguments*

Are the Success and Failure Approaches to Risk Assessment new?

- From a safety perspective, the *success* approach is new in ATM – the *failure* approach is not new!
- Functionality and performance aspects of ATM system behaviour have also been addressed in the past but largely from an "operational" perspective – eg "OPA" in EUROCAE doc ED-78A
- What is new is inclusion of this operational perspective within the scope of risk assessment to form the *success* approach.
- *Success* approach is mentioned in the SAM (with some amplification given in the SCDM) but very limited guidance on it is given therein

EUROCONTROL

What is meant by "ATM directly contributing to an accident" in ESARR 4?

- *"Safety is the top priority in aviation. The main purpose of … ATM services is to ensure the safe separation of aircraft in the air and on the ground, while maintaining the most efficient operational and economic conditions. … ATM services are rarely implicated in fatal aviation accidents. However, the ATM community remains at the forefront of initiatives aimed at improving aviation safety"* - EUROCONTROL website

- We should therefore interpret ESARR 4 as:
  - maximizing the *success* of ATM in <u>preventing</u> aviation accidents that would otherwise have happened
  - not just minimizing accidents (or incidents) <u>caused</u> by *failure* of ATM and that would otherwise <u>not</u> have happened

How should Safety Assessments be documented?

- Individual safety assessment reports on, for example:
  - *a priori* risk assessment processes - eg risk modelling, design analysis, simulations, failure analysis – etc (through FHA, PSSA, SSA)
  - safety monitoring and incident investigation / corrective action

- Safety Case report to bring all the main findings of the individual reports together in a single document in order to:
  - show, in a clear unambiguous way, that an acceptable level of safety is being (or will be) achieved

Why use a Safety Case?

"The prime responsibility for the safety of an ATM service rests with the service provider. Within the overall management of the service, the service provider has a responsibility to ensure that all relevant safety issues have been satisfactorily dealt with and to provide ***assurance*** *that this has been done" –* ESARR 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 …(a). that correct and complete* ***arguments*** *are established to demonstrate that the constituent part under consideration, as well as the overall ATM System are, and will remain, tolerably safe including, as appropriate, specifications of any predictive, monitoring or survey techniques being used –* ESARR 4

*"****Primarily*** *the Safety Case is a matter of ensuring that every company produces a formal safety assessment to* ***assure itself*** *that its operations are safe -* Lord Justice Cullen in his report on the investigation into the Piper Alpha Oil Platform accident

What is a Safety Case?

- Evolved from the Legal Case
- Comparison with Legal Cases:
  - ☑ Argument and Evidence - in safety work, Argument + Evidence = Assurance
  - ☑ Case for the "Defence"
  - ☑ Argument is paramount - basis for whole Safety Case
  - ☑ Rules of Evidence apply - much of it comes from safety assessments etc

☒ **Burden of proof rests with the "Defence" !!!**

EUROCONTROL

What Cullen had in mind!

Safety Cases - When and What ??

- When necessary to demonstrate the ***on-going*** safety of a operation, service and/or system [*Unit* Safety Case]

What ESARR 4 has in mind!

- When a significant ***change*** is going to be made to that operation, service and/or system [*Project* Safety Case]

- Relationship is crucial:
  - USC provides ***baseline*** for change
  - PSC ***updates*** the USC after change

Nevertheless, a **very** good idea!

There is no explicit regulation requiring a USC!!

EUROCONTROL

I have an SMS – do I need a USC?

- Safety Management System:
  - "a systematic and explicit approach to defining the **activities** by which safety management is undertaken by an organization in order to achieve acceptable safety" – ESARR 3
- an SMS:
  - defines what is acceptably safe in the local context
  - describes the specific **responsibilities** and **procedures** for demonstrating that an acceptable level of safety is being achieved
- A Unit Safety Case (USC) is one, way of documenting the **results** of applying the SMS processes

SMSs and USCs are complementary - both are needed

EUROCONTROL

Other FAQs to be addressed in later Sessions

- What is the relationship between a **Safety Plan** and a Safety Case?
- Where do **Assurance Levels** fit into the picture?
- What is the relationship between a **Human Factors Case** and a Safety Case?

Mini Exercise – USC

EUROCONTROL

Tasks

- Assume that you are the Safety Manager of an ATSU
- Head of Unit is concerned about his safety accountabilities and wants advice

1. Develop an outline brief for the Head of Unit, to explain :
   - why the Unit should have a USC
   - what should go into a USC
2. Present your findings to the group

Caution!
RVSM is a Safety Case for a change

- Suggestions:
  - Start with the RVSM structure (overleaf) and modify / expand it
  - Decide top-level **claim**
  - Set **objectives** (or arguments) to satisfy claim
  - Suggest the **processes** etc by which the objectives could be achieved

EUROCONTROL

Definition:
Risk of an accident:
1 Within TLS
2 is no higher than pre-RVSM;
and
3 has been reduced AFARP

Claim
RVSM is
acceptably safe.

Context
ECAC airspace only

Obj 1
RVSM has been specified to be *acceptably safe*

▽ [tbd]

Obj 2
RVSM will be implemented in accordance with the specification

▽ [tbd]

Obj 3
The Switchover to operational service of RVSM will be *acceptably safe*

▽ [tbd]

Obj 4
The safety of RVSM will continue to be demonstrated in operational service

▽ [tbd]

EUROCONTROL

This is only an **OUTLINE**!!

USC – Suggested Solution

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

Cr001
Acceptably safe means:
- Safety Targets for services are met; and
- risk of an accident is reduced AFARP

Obj 0
ATM services provided by ATSU[X] are, and will remain, *acceptably safe*

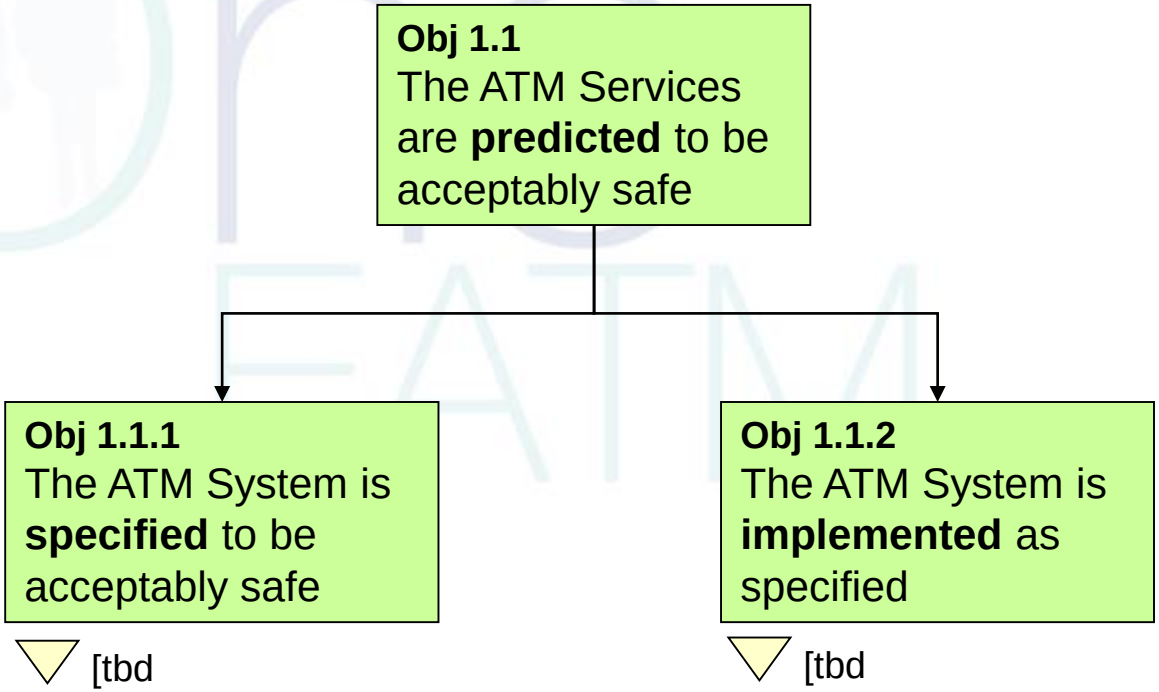
C001
Applies to the extant system configuration

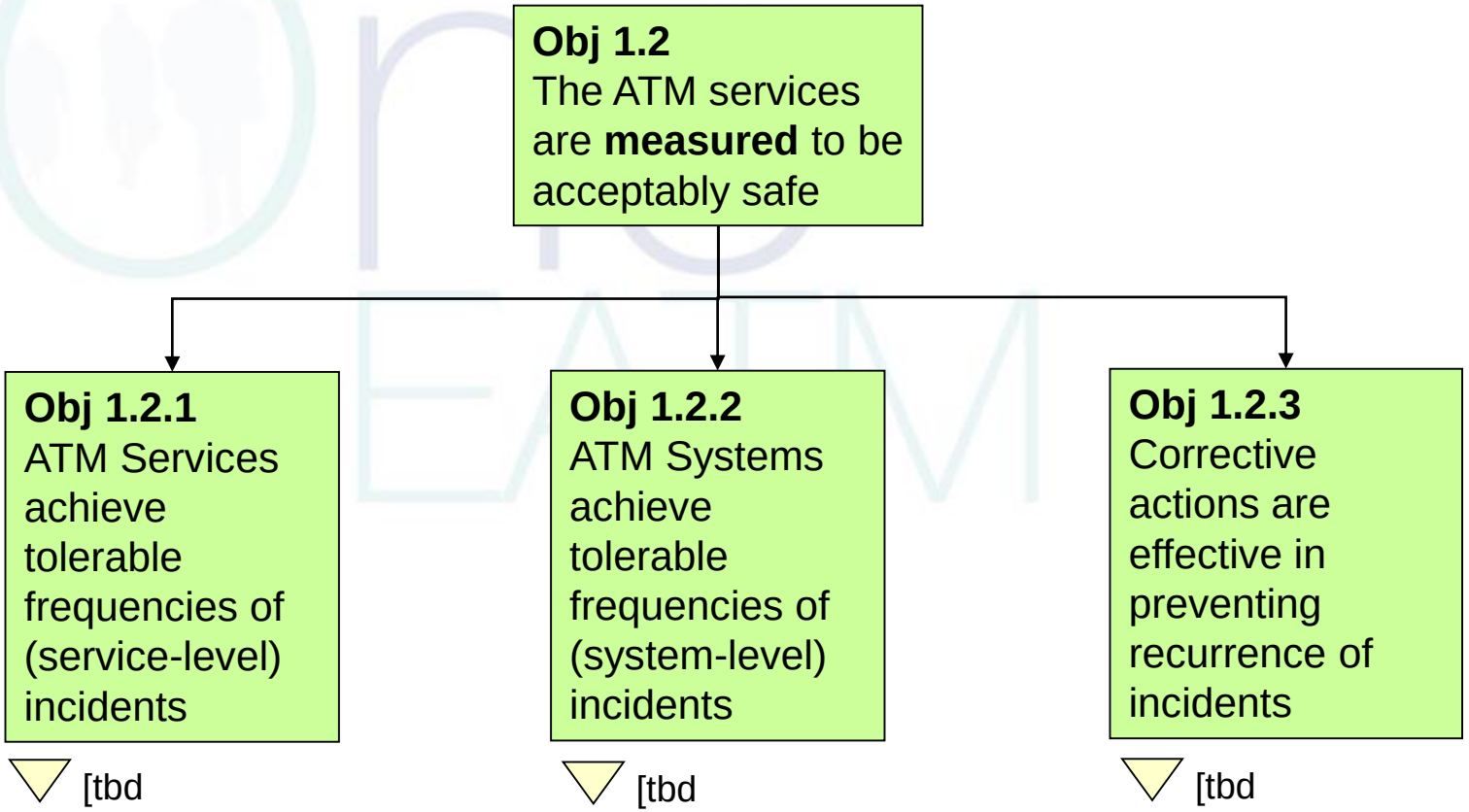
Obj 1
The on-going ATM Services are acceptably safe

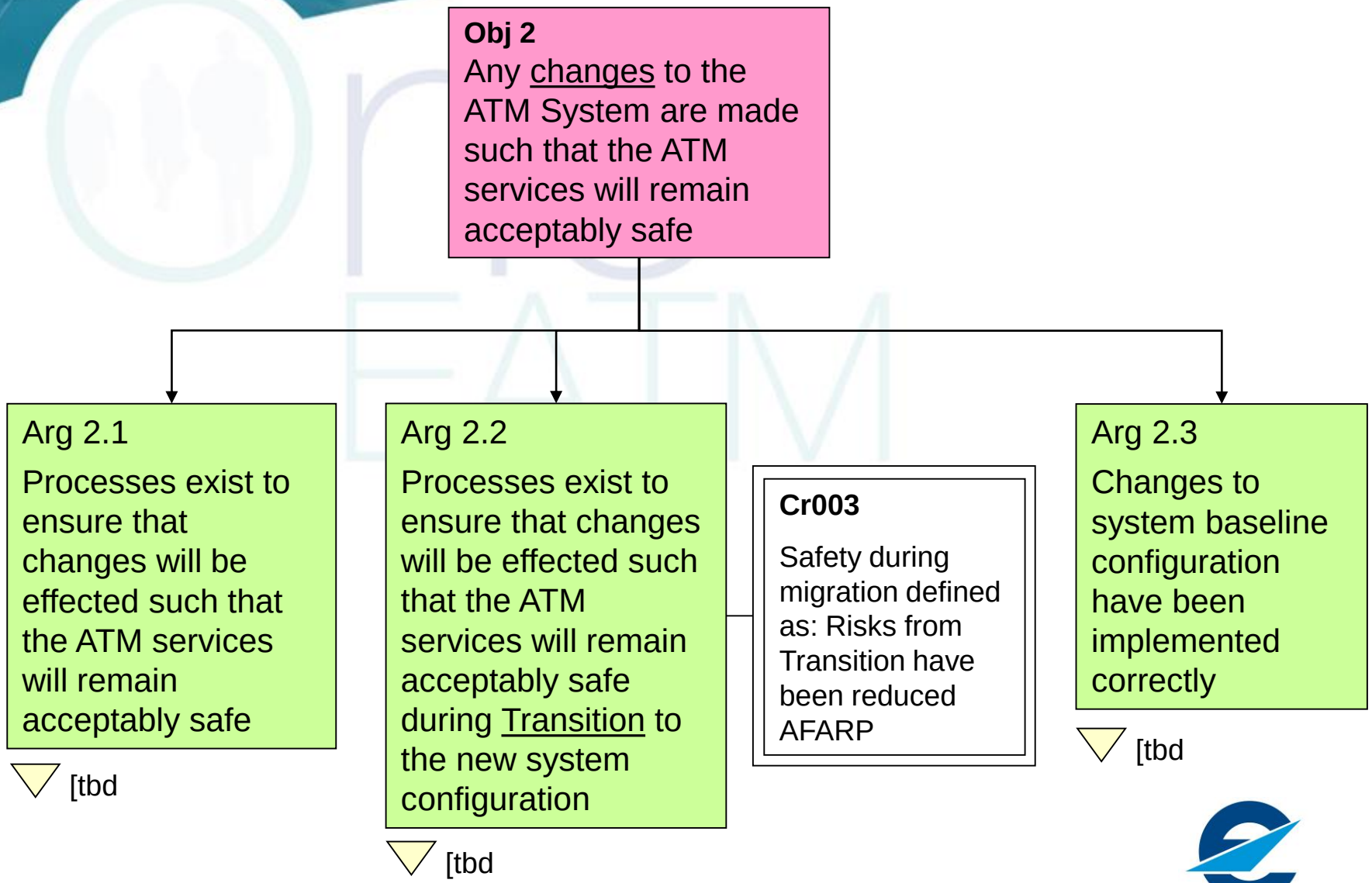
Obj 2
Any changes to the ATM System will be made such that the ATM services will remain acceptably safe

Obj 1.1
The ATM Services are **predicted** to be acceptably safe

Obj 1.2
The ATM Services are **measured** to be acceptably safe


Obj 1.1
The ATM Services are **predicted** to be acceptably safe
Obj 1.1.1
The ATM System is **specified** to be acceptably safe
[tbd
Obj 1.1.2
The ATM System is **implemented** as specified
[tbd


Obj 1.2
The ATM services are measured to be acceptably safe
Obj 1.2.1
ATM Services achieve tolerable frequencies of (service-level) incidents
[tbd
Obj 1.2.2
ATM Systems achieve tolerable frequencies of (system-level) incidents
[tbd
Obj 1.2.3
Corrective actions are effective in preventing recurrence of incidents
[tbd


Obj 2
Any changes to the ATM System are made such that the ATM services will remain acceptably safe
Arg 2.1
Processes exist to ensure that changes will be effected such that the ATM services will remain acceptably safe
[tbd
Arg 2.2
Processes exist to ensure that changes will be effected such that the ATM services will remain acceptably safe during Transition to the new system configuration
[tbd
Cr003
Safety during migration defined as: Risks from Transition have been reduced AFARP
Arg 2.3
Changes to system baseline configuration have been implemented correctly
[tbd

1.1.1 ATM System Specified to be Safe

- Safety Targets set for design
- Unit-level FHA to derive “Safety Functions” and set Safety Objectives
- Unit-level PSSA to derive Functional Safety Requirements and Safety Integrity Requirements for ATM system (people, procedures and equipment)
- Analysis to show that Safety Requirements satisfy the Safety Targets
- Unit-level FHA and PSSA updated periodically to reflect changes

1.1.2 ATM System Implemented as Specified

- Unit-level SSA:
  - Safety Requirements from Unit-level PSSA allocated and apportioned to physical system
  - Physical Safety Requirements expanded as required
- Direct Evidence of satisfaction of Safety Requirements for:
  - People – including training
  - Procedures
  - Equipment
  - Interactions between these three
- Indirect Evidence from Safety Assurance processes

See later Sessions !!

1.2.1 & 1.2.2 Safety Achievement

- Safety indicators set for Safety Monitoring
- Operational incident monitoring against Safety Indicators, in accordance with ESARR 2
- Equipment incident monitoring against Safety Indicators, in accordance with ESARR 2
- Equipment reliability analysis against predictions
- etc

1.2.3 Incident Reporting, Investigation and Corrective Actions

- Process for encouraging the reporting of safety incidents
- Culture for encouraging the reporting of safety incidents
- Surveys showing that the incident-reporting processes and culture are effective
- Process for investigating incidents
- Audits showing that reported safety incidents are investigated effectively
- Process for Corrective Actions
- Audits showing that Corrective Actions from incident investigations are implemented throughout the ATSU
- Effectiveness of Corrective Actions demonstrated through monitoring and trend analysis

2.1 Process for Managing Change

- Generic set of safety-management and related processes to ensure the safety of changes to the ATM system – in accordance with ESARR 4
- Procedures for establishing the scope and safety significance of specific changes
- Procedures for selecting the appropriate safety-management and related processes for specific changes
- Audits to show that the safety-management and related processes, selected for specific changes, have been followed correctly
- etc

Incorporated in Ops, Eng and Safety Management manuals

EUROCONTROL

2.2 Transition to new System Configuration

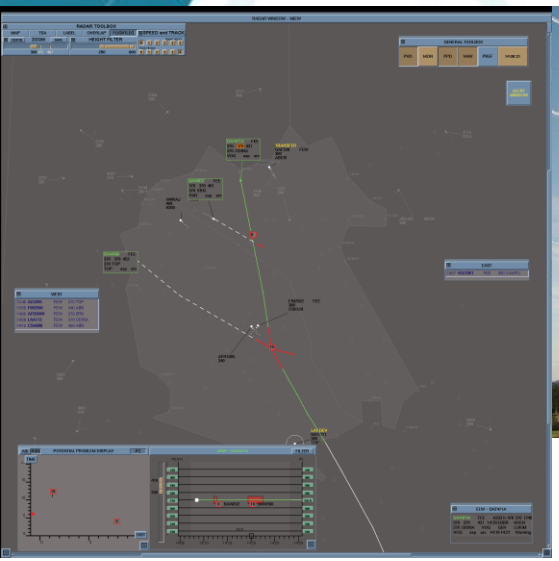
- Procedures for bring the changes into service, and in-service support. Include:
  - publication of operational procedures, airspace changes (if any), publication of engineering procedures, provision of resources (people, equipment spares, maintenance facilities etc) and training of operational and technical personnel
  - arrangements for safety management, change management, configuration control etc
- Procedures for switching over from the old systems to the new systems. Include:
  - switchover procedures, allocation of responsibilities and training / briefing of personnel.
- Procedures for identifying and mitigation hazards associated with switch-over from the old systems to the new systems. Include:
  - a sort of FHA/PSSA/SSA of the switchover
  - additional procedures, allocation of responsibilities and training / briefing of personnel necessary to prevent (as far as possible) things going wrong
  - Fallback procedures should something go wrong
- etc

EUROCONTROL

2.3 Implementation of Changes to System Baseline

- Project Safety Cases
- Other change-acceptance records
- Safety audits against system-change processes
- etc

Questions ??



?

EUROCONTROL