Safety Assurance in the Safety Lifecycle

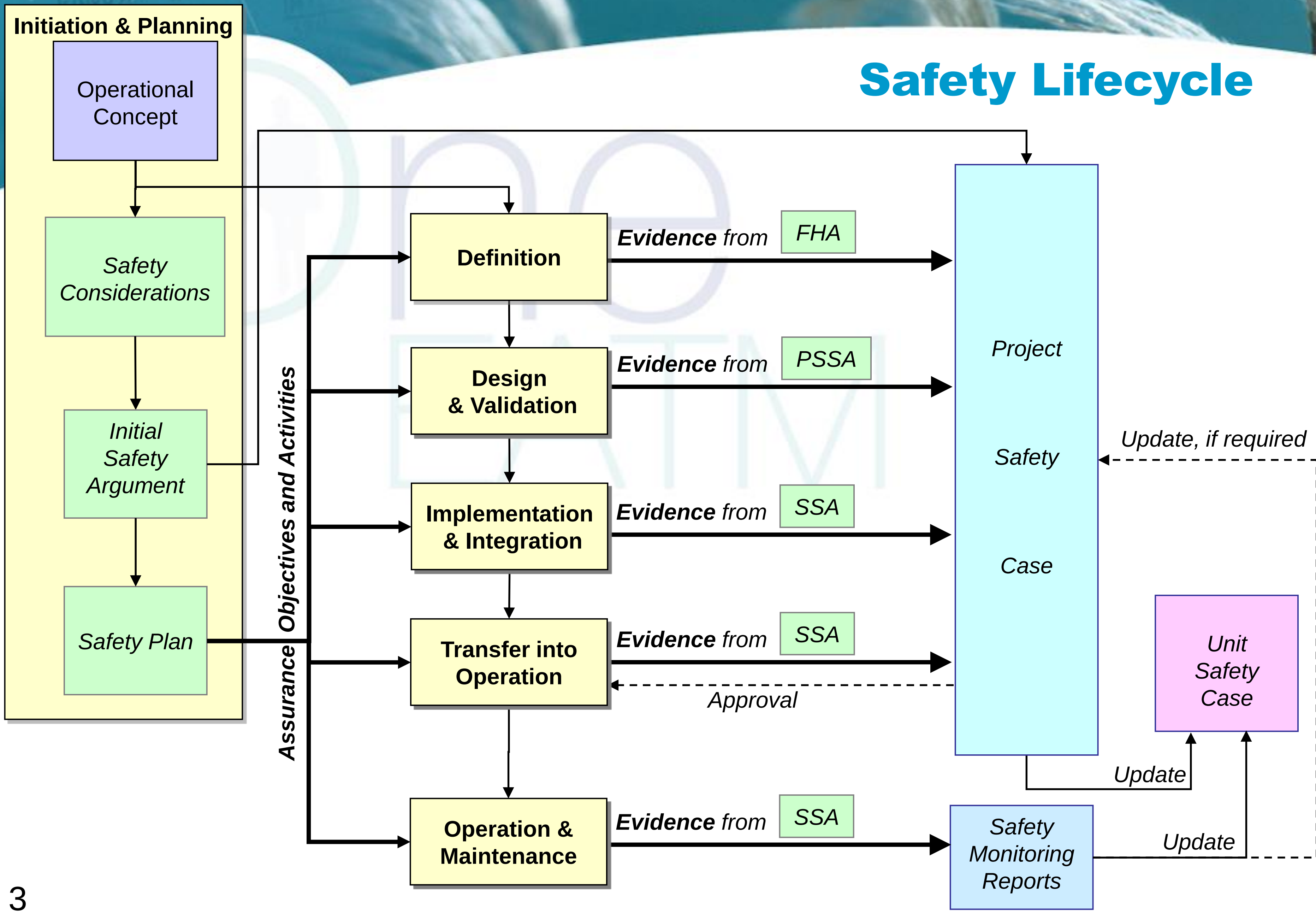
Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL Safety Assessment Methodology

- Defines three assessment stages:
  - Functional Hazard Analysis (FHA)
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)
- The broader approach proposed by Safety Assessment Made Easier:
  - incorporates the Success approach
  - extends the scope of FHA, PSSA and SSA accordingly

Safety Lifecycle



Safety Considerations

- First stage for a project, after Operational Concept:
  - identify where project needs to have / may have an impact on safety (positive or negative)
  - decide if the project needs a formal Safety Plan or not
  - decide appropriate Safety Criteria
  - outline what needs to be done to ensure that the project is ‘safe’
- Where appropriate, supported by:
  - “What is a Change?” - see [**SAM guidance**]
  - *Human Factors Fact Finding* - see [**HF Case**]
  - Safety Considerations Checklist - to be produced and incorporated in [***SAME***] – meanwhile see [**EEC Booklet**]
- **Not** “done and forgotten”
  - issues identified must be captured as System-level Safety Assurance Objectives / Activities

Safety Criteria – the need

- A Safety Argument always starts with the (top-level) Claim that something is *safe*
- Safety Criteria provide meaning to top-level Claim – by defining what is *safe*
- They should also determine:
  - the form of the Safety Argument
  - the form of the related Safety Assessment process

Safety Criteria - types

- Absolute:
  - eg compliance with a TLS
- Relative:
  - eg "risk is no higher than…"
  - eg "risk is substantially lower than …"
- Reductive:
  - eg "risk is reduced AFARP" [ESARR 3, paragraph 5.1.4]

Which is / are appropriate, and when?

Should be addressed in Safety Considerations

Safety Criteria - sources

- Absolute TLSs include:
  - OCP TLS: 1e-7 per approach for precision approaches, failure-free case only
  - RVSM TLS: 5e-9 per flt hr for vertical dimension, for all causes
  - Risk Classification Schemes
  - specific targets derived from, for example, [**IRP**]

See [**SCDM**] and [**ED-125**]

- ATM 2000+ states that risk shall not increase, and preferably decrease [relatively]
  - ESARR 4 “TLS” is numerical interpretation of ATM 2000+, thus is a relative criterion in disguise!
- Reducing risk AFARP is an obligation on ANSPs:
  - ESARR 3, paragraph 5.1.4

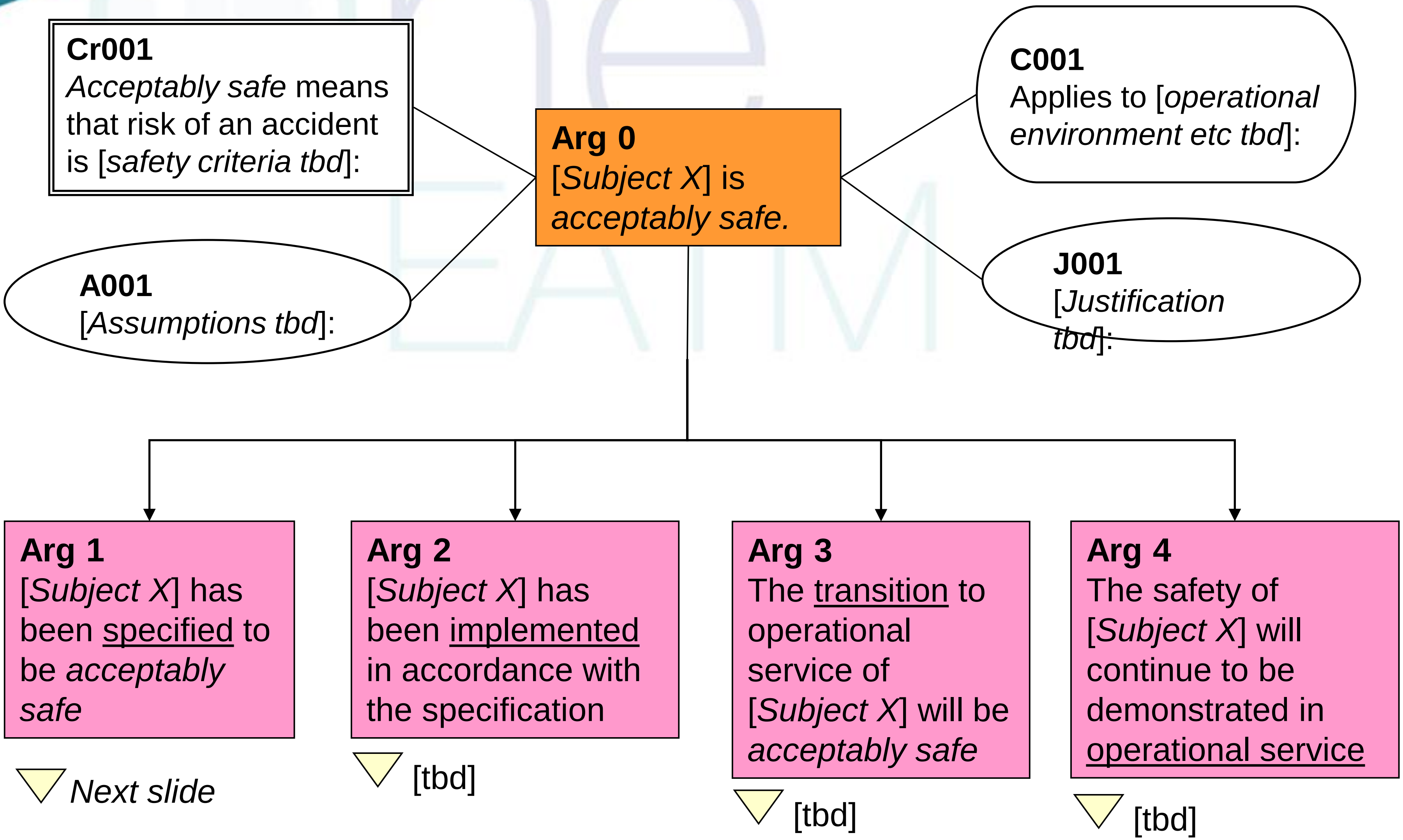
EUROCONTROL

Safety Argument

- Builds on Safety Considerations
- As complete as possible at initial stage:
  - at least sufficient to provide framework for Assurance Objectives
  - but recognize that it may need to change as Project develops
- Good idea to discuss with Safety Regulator – reduce risk of regulatory objections later !

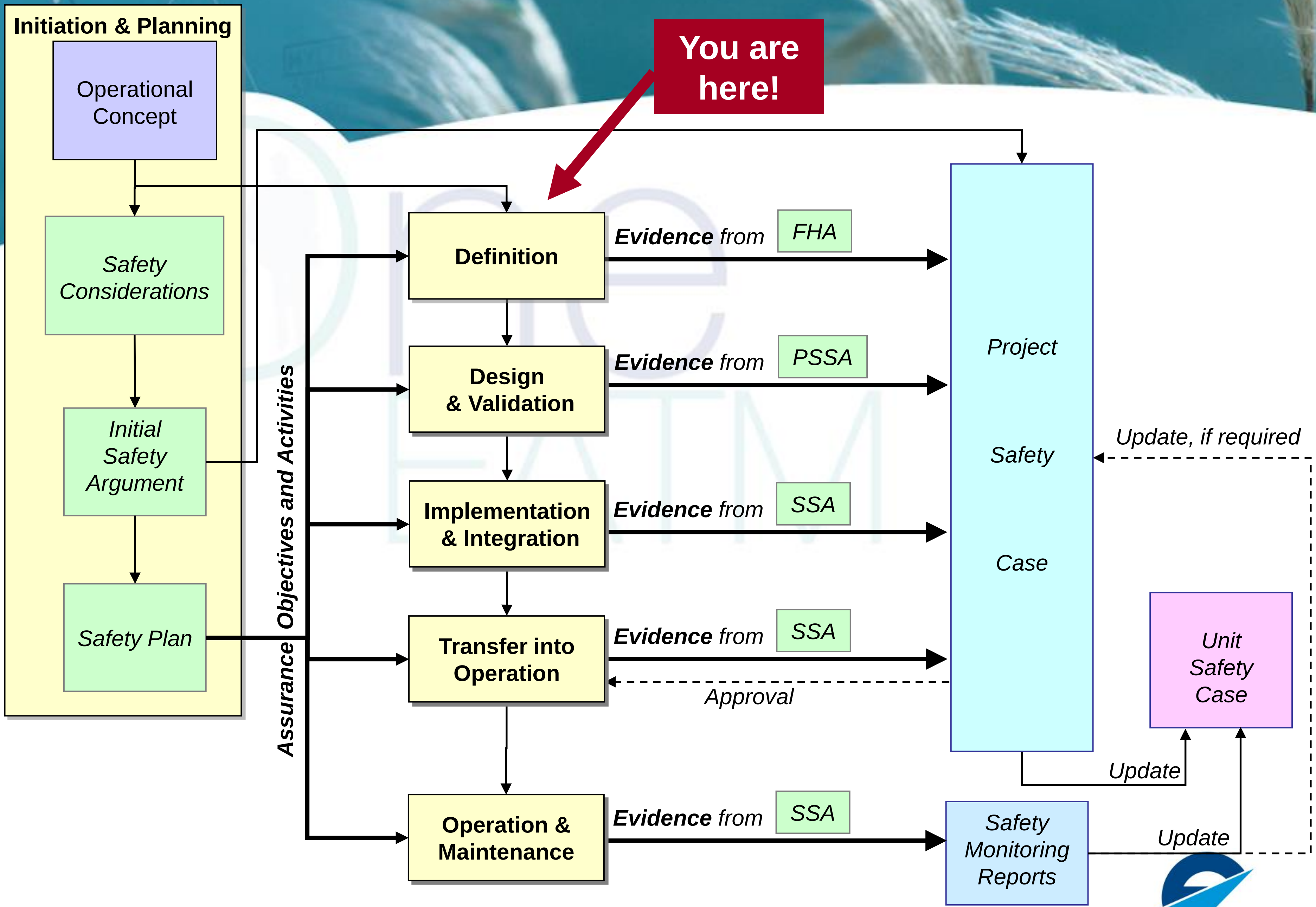
EUROCONTROL

Top-level Safety Argument for a "Change"



Safety Plan

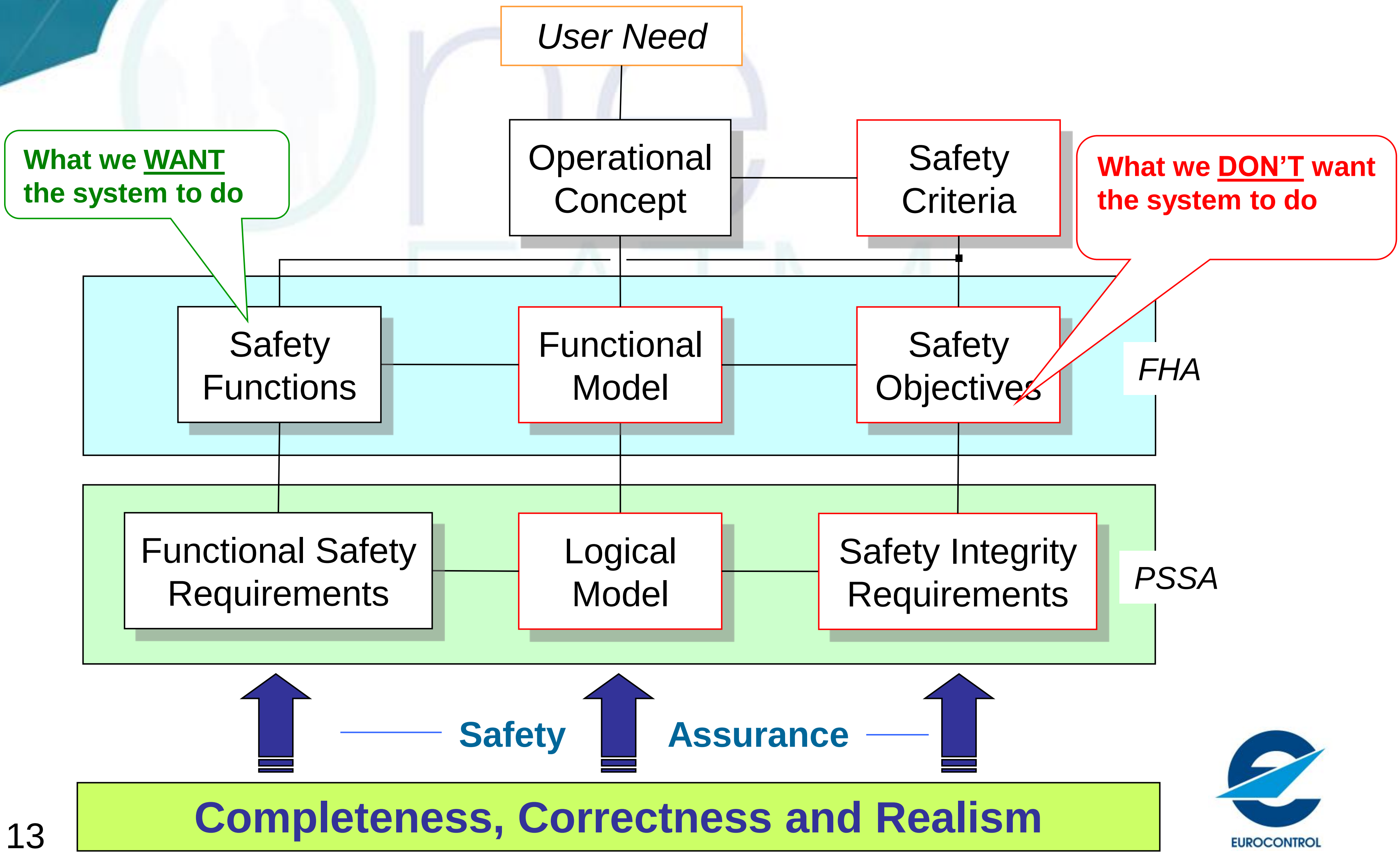
- Builds on / structured around the Safety Argument
- Specifies how the Argument will be addressed - eg the:
  - Further decomposition of the Argument
  - Safety Assurance Objectives to satisfy each strand of the Argument
  - Safety Assurance Activities – how each Assurance Objective will be achieved
  - Evidence to be produced by each Activity
- Should incorporate safety-related issues from the Safety Considerations process (including HF Fact Finding, where applicable)
- Should incorporate safety-related issues from the *HF Issues Analysis*, - see [**HF Case**] - as Safety Assurance Objectives / Activities
- Specifies safety responsibilities, resources and schedule of Activities



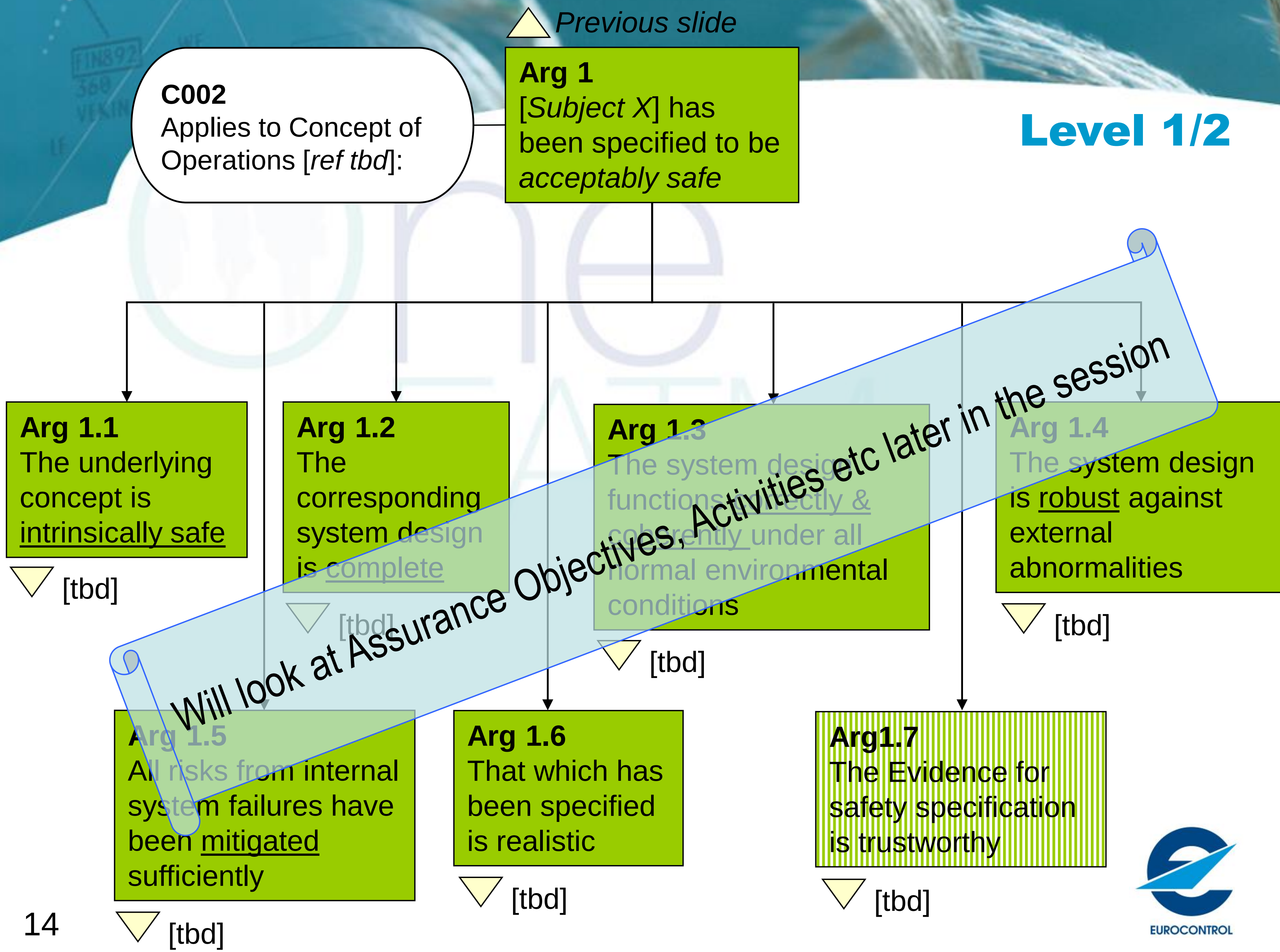
Initiation & Planning
Operational Concept
Safety Considerations
Initial Safety Argument
Safety Plan
You are here!
Assurance Objectives and Activities
Definition
Design & Validation
Implementation & Integration
Transfer into Operation
Operation & Maintenance
Evidence from
FHA
Evidence from
PSSA
Evidence from
SSA
Evidence from
SSA
Evidence from
SSA
Approval
Project Safety Case
Update, if required
Unit Safety Case
Update
Safety Monitoring Reports
Update
EUROCONTROL

Design and Definition Phases

Definition & Design Phases



Level 1/2

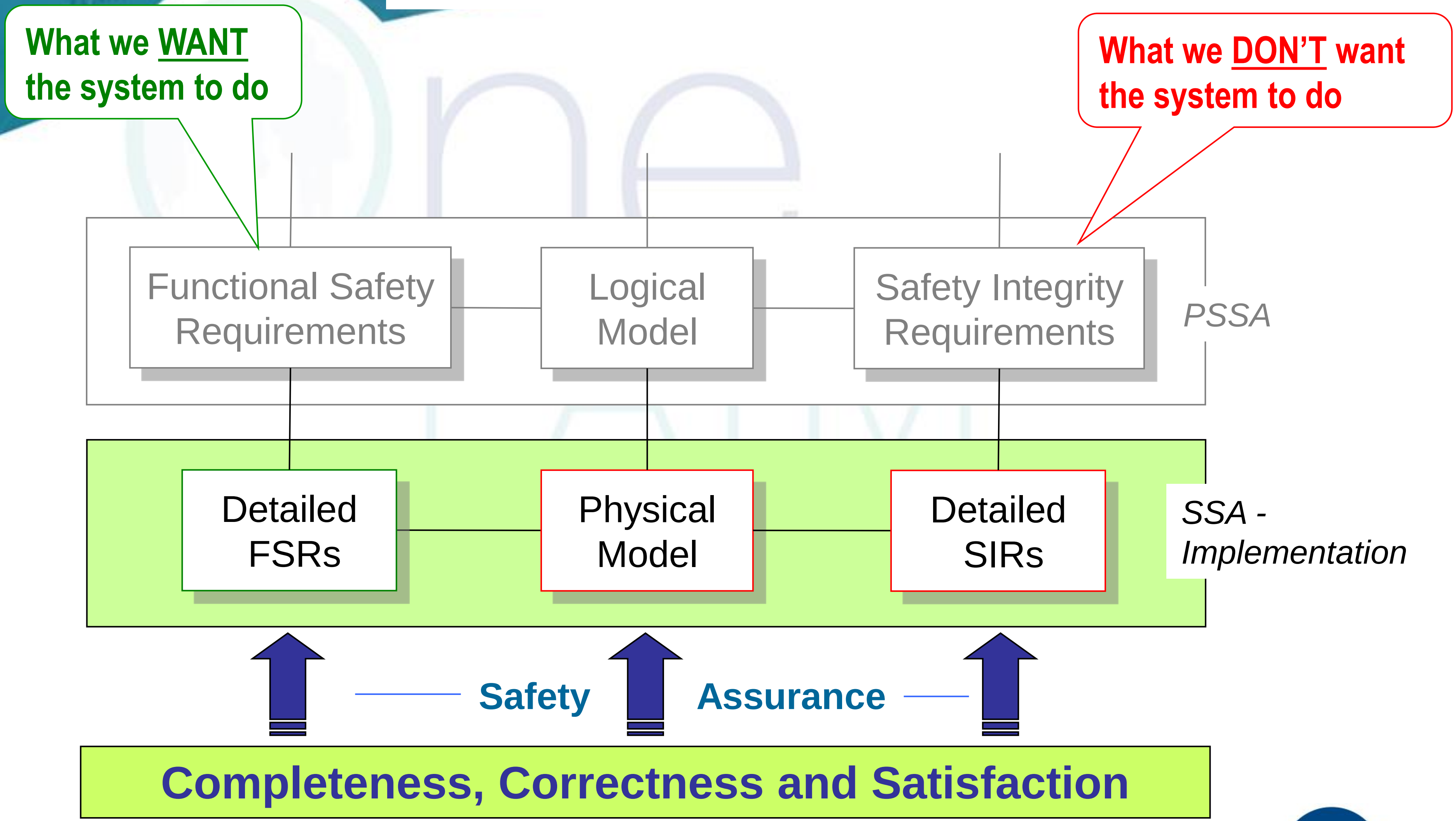

Previous slide
C002
Applies to Concept of Operations [ref tbd]:
Arg 1
[Subject X] has been specified to be acceptably safe
Arg 1.1
The underlying concept is intrinsically safe
[tbd]
Arg 1.2
The corresponding system design is complete
[tbd]
Arg 1.3
The system design functions correctly & coherently under all normal environmental conditions
[tbd]
Arg 1.4
The system design is robust against external abnormalities
[tbd]
Arg 1.5
All risks from internal system failures have been mitigated sufficiently
[tbd]
Arg 1.6
That which has been specified is realistic
[tbd]
Arg1.7
The Evidence for safety specification is trustworthy
[tbd]
Will look at Assurance Objectives, Activities etc later in the session

Implementation and Integration Phases

Not yet covered in *SAME*

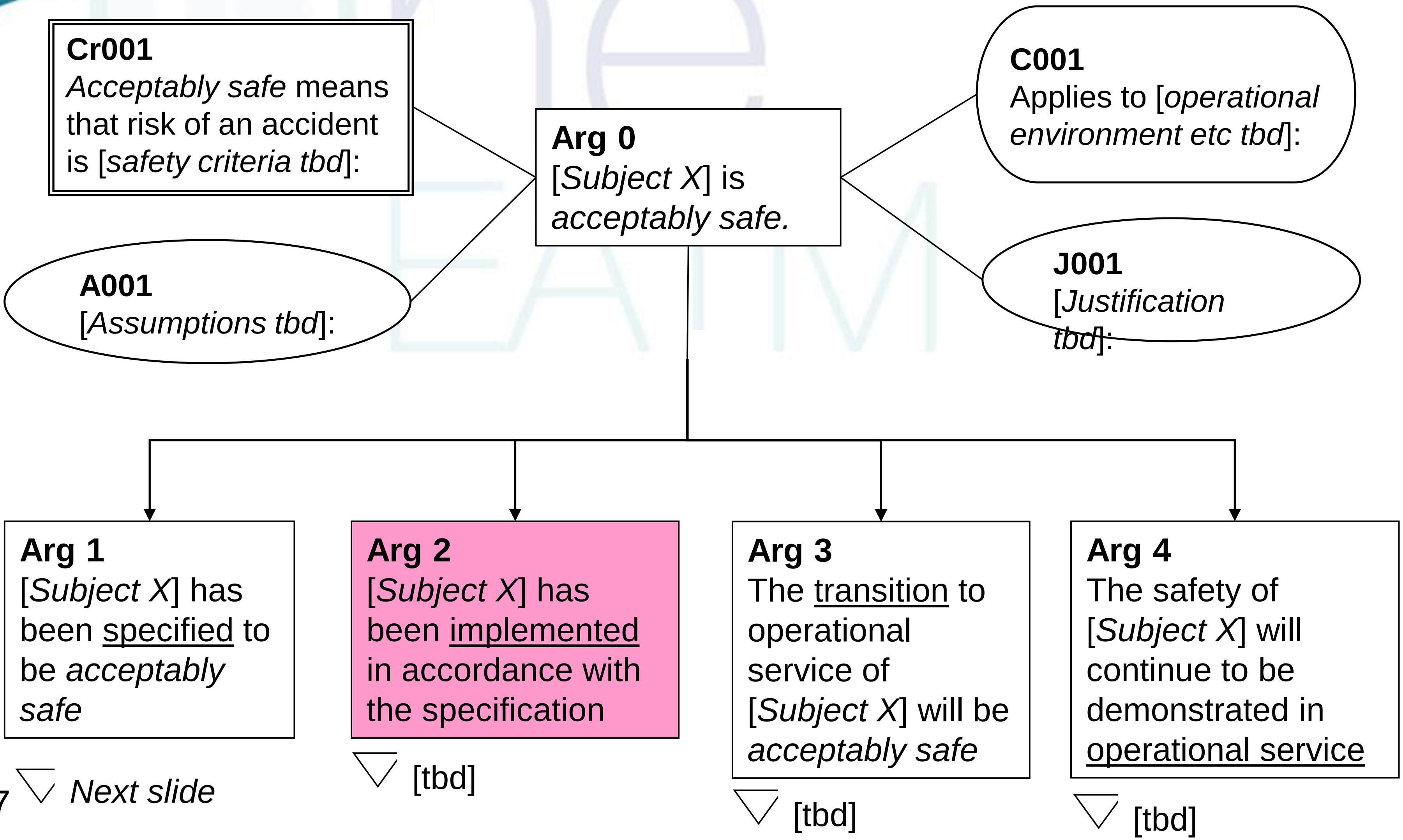
Overview

Implementation & Integration Phases



EUROCONTROL

Top-level Safety Argument for a "Change"



Implementation & Integration Key Points (1)

- Addresses whether the physical system as built achieves the required level of safety
- Should provide sufficient Evidence to satisfy Arg2 (via lower-level, sub-Arguments)
- Covers a substantial part of the [**SAM**] **SSA** process
- Proving System Functionality & Performance:
  - prove completeness and correctness of detailed Safety Requirements (similar to Design & Definition)
  - prove satisfaction of detailed Safety Requirements – mainly test and operational evaluation / trials (normal and abnormal conditions
  - very important to include reversionary modes of operation

Implementation & Integration Key Points (2)

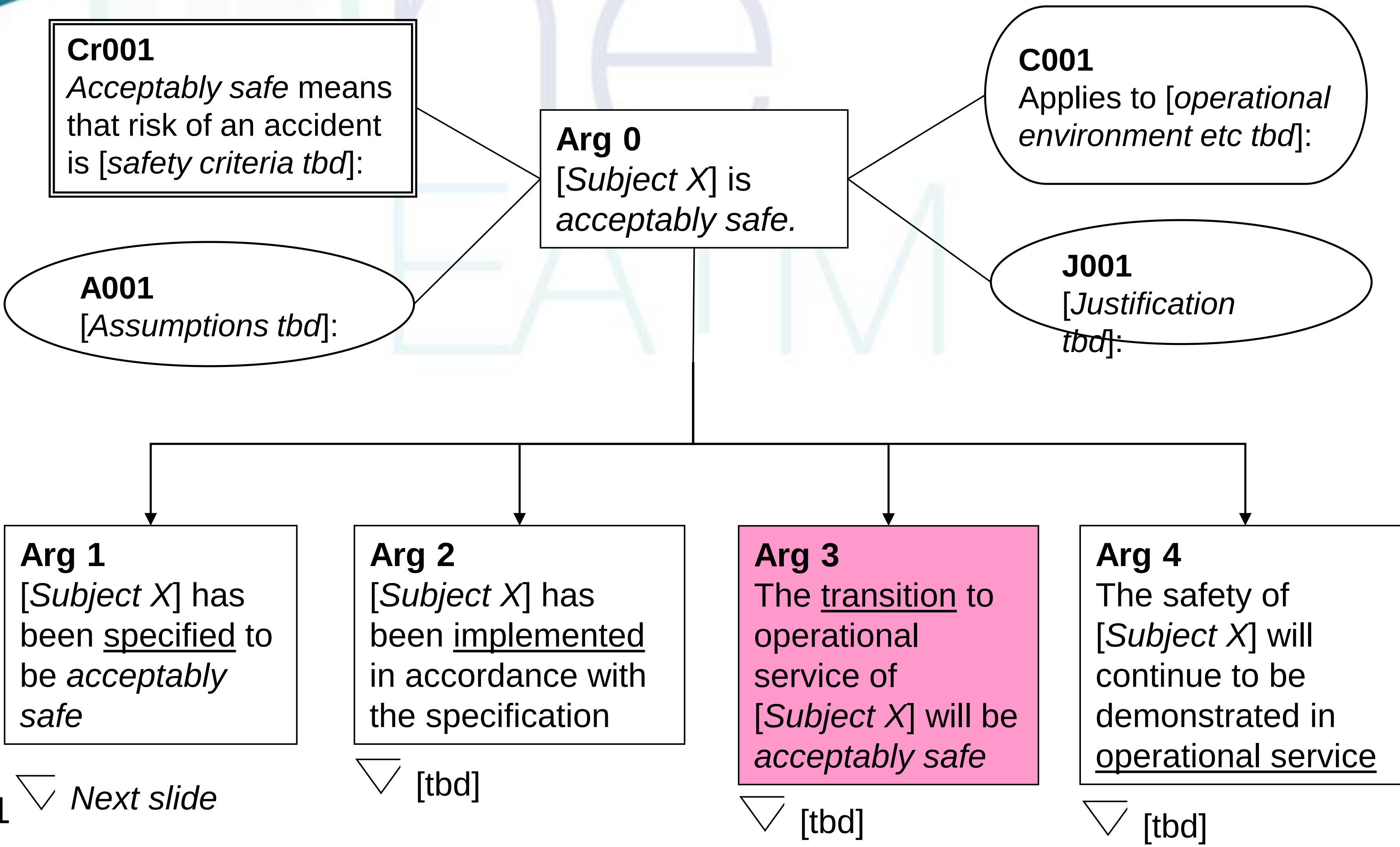
- Proving System Reliability & Integrity:
  - derive a set of detailed Safety Integrity Requirements for the physical architecture
  - show that these detailed Safety Integrity Requirements satisfy those specified in the PSSA for the logical architecture
  - show that no undesired properties of the system have emerged in the physical design and/or system as built
- Problem with confidence in Safety Integrity Requirements satisfaction evidence – therefore use:
  - Evidence from PSSA that the Safety Integrity Requirements are realistic – ie are capable of being satisfied in a typical implementation similar to the one proposed
  - ***Assurance-level*** approach to provide confidence that they have been satisfied – see later this Session

Transfer-to-Operation Phase

Not yet covered in *SAME*

Overview

Top-level Safety Argument for a "Change"



Transfer into Operation - Key Points

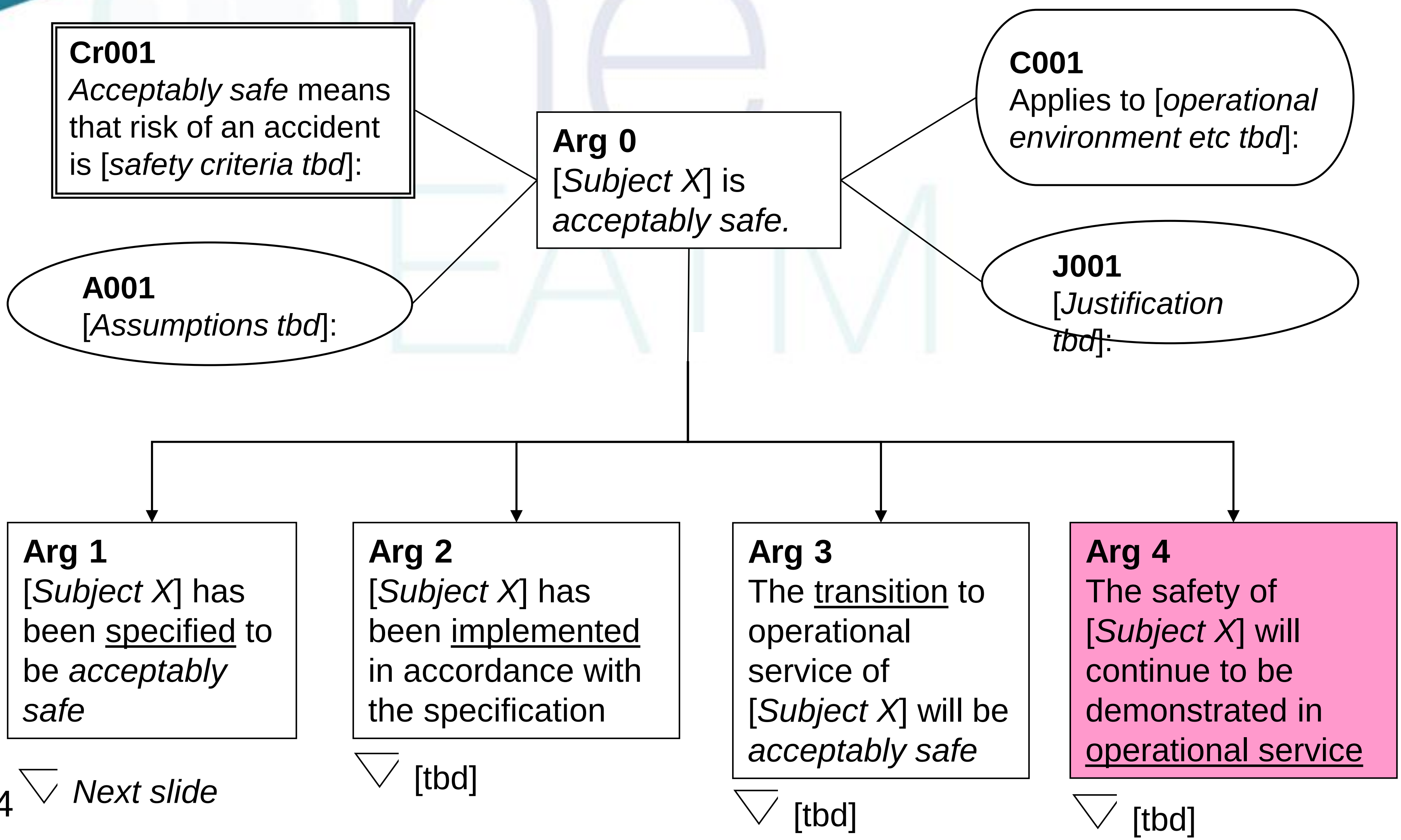
- Addresses whether the fully proven system:
  - is <u>ready</u> to be brought into operational use, and
  - without <u>degrading</u> the continuity and safety of the on-going ATM service
- Should provide sufficient Evidence to satisfy Arg3 (via lower-level, sub-Arguments)
- Covers the second part of the [**SAM**] **SSA** process
- Need to show that:
  - all preparations for bring the individual systems / subsystems in to service, and for supporting them in service, have been completed
  - process of switching over from the old systems to the new systems has been fully planned and resourced
  - all hazards associated with switch-over from the old systems to the new systems have been assessed and mitigated sufficiently

Operation-and-Maintenance Phase

Not yet covered in *SAME*

Overview

Top-level Safety Argument for a “Change”

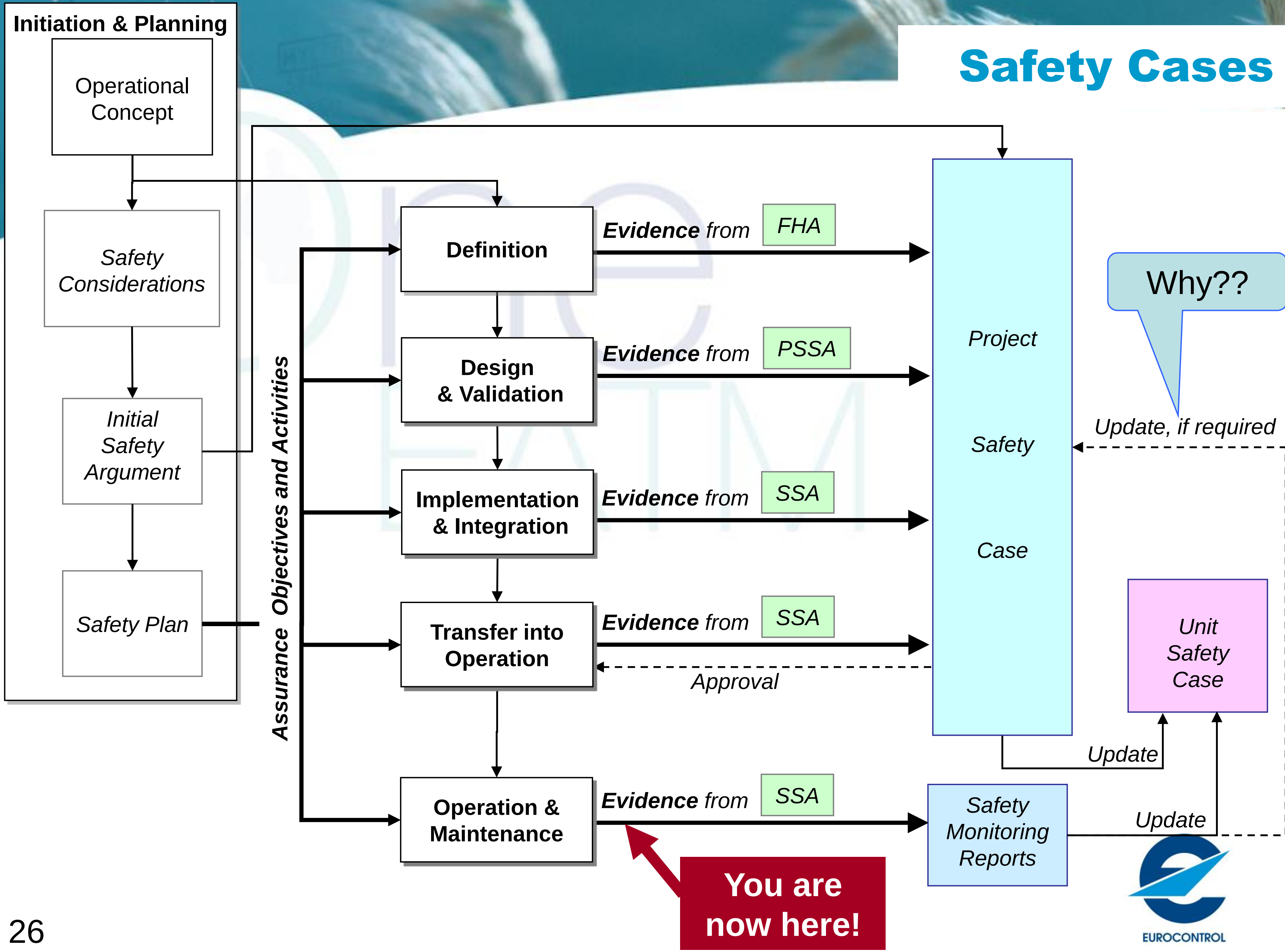


Operation & Maintenance - Key Points

- Addresses in-service monitoring of the safety of the system
- Should provide sufficient Evidence that the physical system in practice achieves an acceptable (or at least a tolerable) level of risk – ie to satisfy Arg4 (via lower-level, sub-Arguments)
- Covers the third part of the [SAM] **SSA** process
- Need to show that:
  - Safety Criteria are met in practice – to validate the *a priori* assessment
  - all safety-related incidents are reported, investigated and the appropriate corrective action taken – important to AFARP criterion
  - safety assessments have been carried out of any maintenance and/or other planned interventions – show that risks are known and accepted

Relevance of the last point??!!

Safety Cases



Safety Case Development Manual

- Now part of SAM V2.1
- Based on practical experience – good and bad!!
- Comprises:
  - Essentials: *Getting Started* and *Argument & Evidence*
  - Guidance: to support *Essentials*
  - Examples (using GSN)
  - Checklist: used by DAP/SSH to review Safety Cases
- Aimed primarily at EATM (including suppliers!!) but a lot of Stakeholders are interested also
- Applies to *Project Safety Cases* and *Unit Safety Cases*

EUROCONTROL

That concludes Part 1 of Safety Assessment Made Easier

Now for an overview of Part 2!

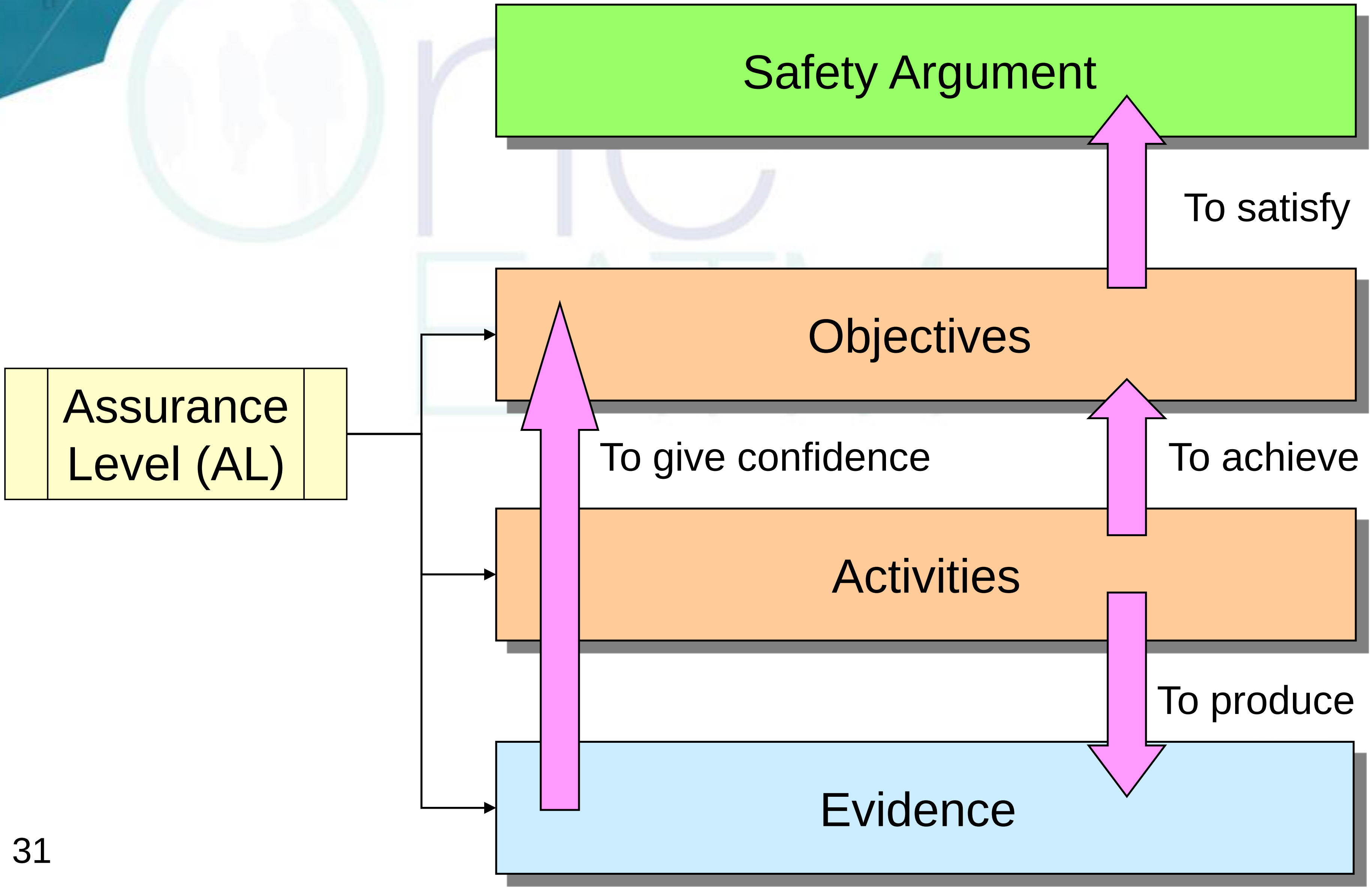
Safety Assurance

Principles and Practice

Why Safety Assurance?

- To strengthen Safety Case:
  - Arguments are only true or false (deliberately so!)
  - Evidence is rarely absolutely conclusive
  - Assurance process tells us: how much, how obtained, how good, etc
- To demonstrate Safety Integrity Requirements satisfaction:
  - Difficult to do through testing alone – issues about software-test coverage, amount of hardware testing (10x MTBF), repeatability of human performance assessment etc etc
  - Show that Safety Integrity Requirements are achievable (in PSSA)
  - Apply specified assurance process in SSA to give indirect Evidence that they have been achieved
  - Content and rigour of assurance processes determined by criticality of system / system-element concerned – **Assurance Levels**

Safety Assurance – general structure



Assurance Levels

- Tailored for ATM:
  - SWAL (Software Assurance Level)
  - PAL (Procedure Assurance Level)
    - Operational procedure
  - HAL for Ops staff (Human Assurance Level)
  - SAL (System-level Assurance
  - Maintenance Intervention Assurance Level

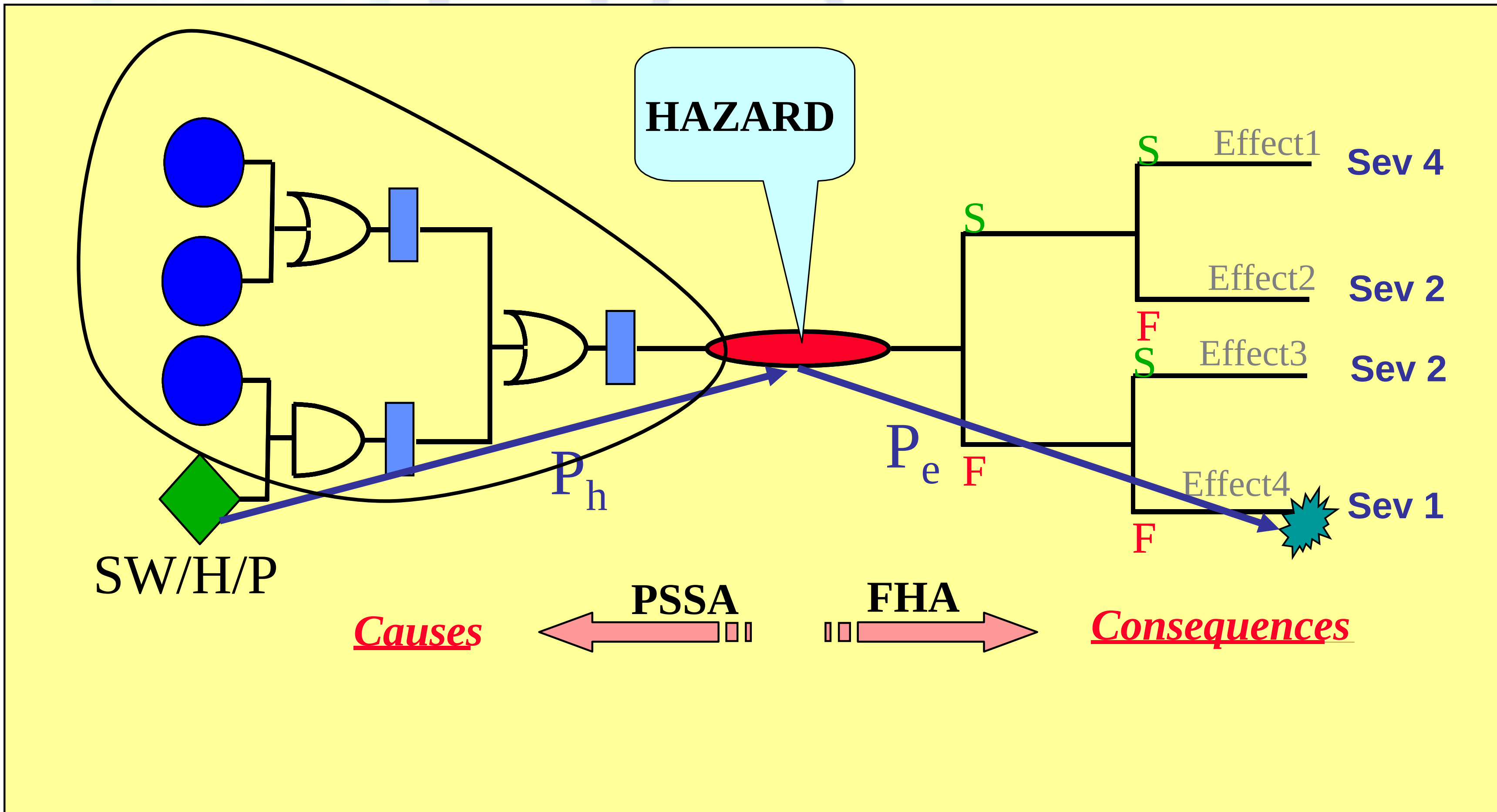
Under development

New but at the core of *SAME*

- Reused from Airborne
  - HWAL (Hardware Assurance Level)

EUROCONTROL

Deriving Assurance Levels (1)



Deriving Assurance Levels (2)

As per ESARR 4

Severity of the Effect / Likelihood of generating such an effect P_e or (P_h x P_e)	1	2	3	4
Very Possible	AL1	AL2	AL3	AL4
Possible	AL2	AL3	AL3	AL4
Very Unlikely	AL3	AL3	AL4	AL4
Extremely Unlikely	AL4	AL4	AL4	AL4

System-level Safety Assurance

For further information on SWALs, PALs and HALs see [**IET 25 ALs**] and [**SAM**]

In Workshop pack!

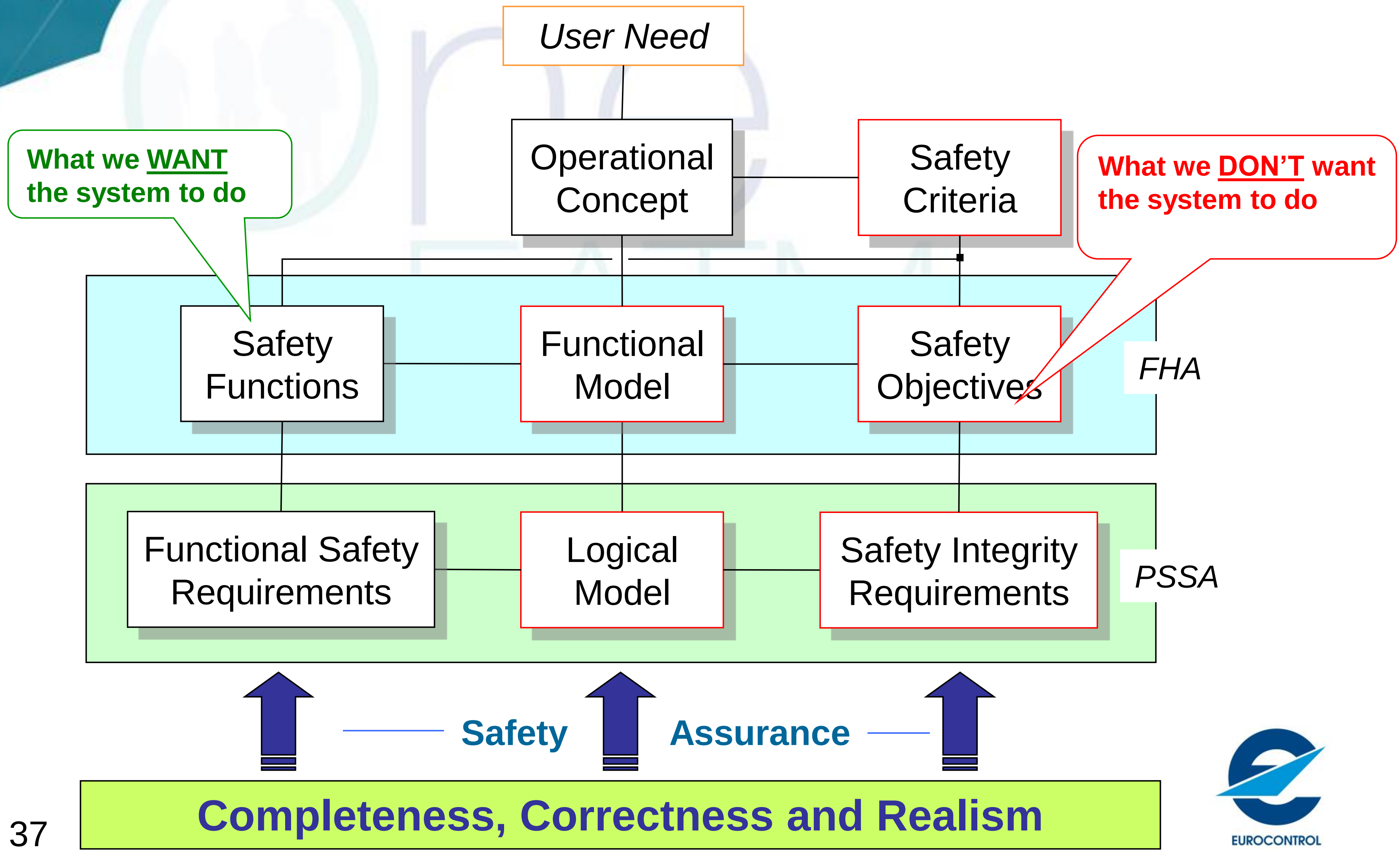
System-level Safety Assurance

- In *SAME* Part 2
- Throughout the lifecycle, we need assurance that the system:
  - has the required **functionality and performance**, and operates as intended,
  - and has the required **integrity**
- Only Design and Definition phases of lifecycle covered at present:
  - we plan to do other phases eventually

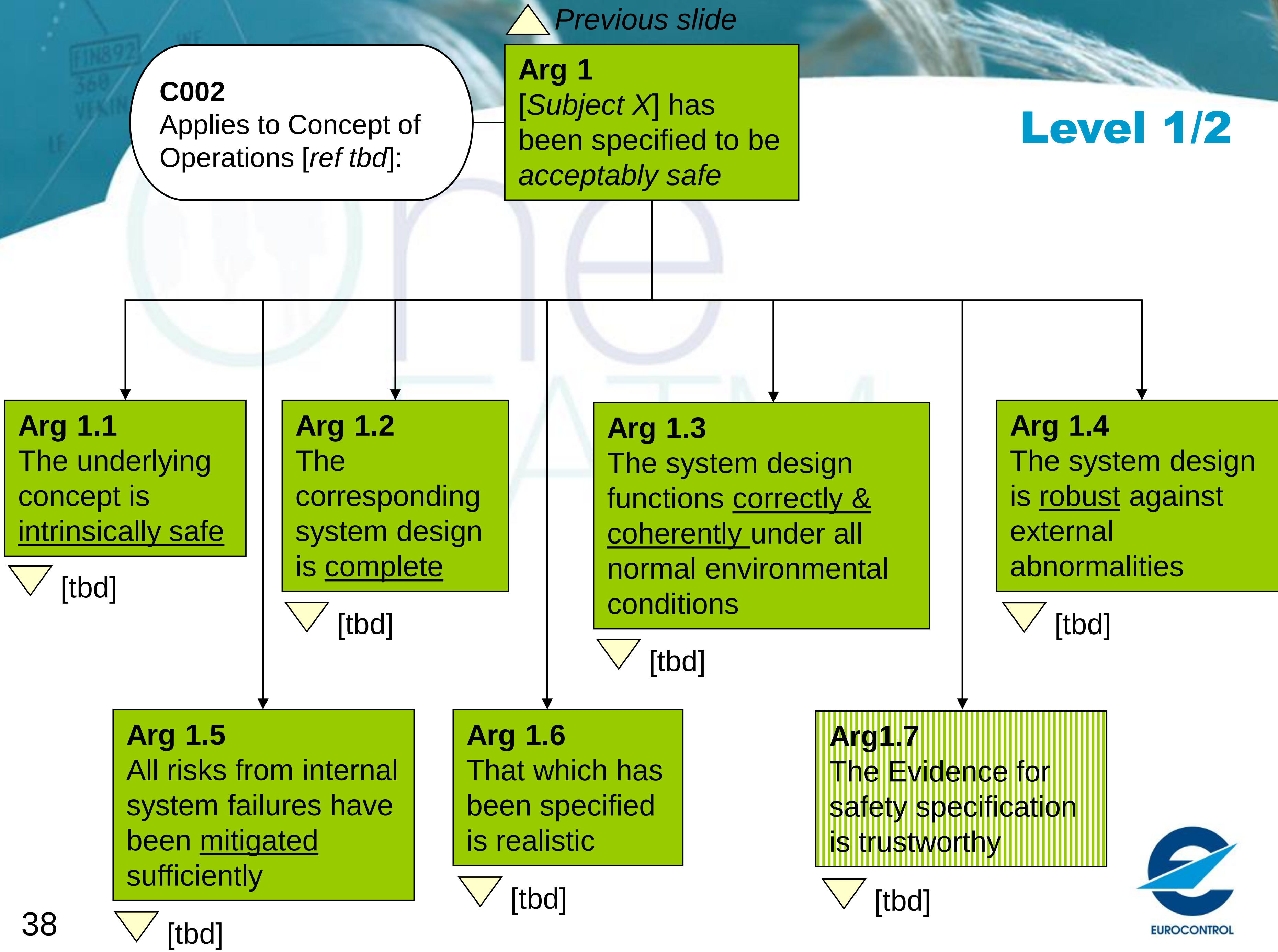
"… the application of good systems-engineering practices to system safety assessment." !!

EUROCONTROL

Definition & Design Phases



Level 1/2


Previous slide
Arg 1
[*Subject X*] has been specified to be *acceptably safe*
C002
Applies to Concept of Operations [*ref tbd*]:
Arg 1.1
The underlying concept is intrinsically safe
[tbd]
Arg 1.2
The corresponding system design is complete
[tbd]
Arg 1.3
The system design functions correctly & coherently under all normal environmental conditions
[tbd]
Arg 1.4
The system design is robust against external abnormalities
[tbd]
Arg 1.5
All risks from internal system failures have been mitigated sufficiently
[tbd]
Arg 1.6
That which has been specified is realistic
[tbd]
Arg1.7
The Evidence for safety specification is trustworthy
[tbd]

So we have...

- The **Safety Argument** – statements to support the **Claim** that something is / will be "safe"
- **Assurance Objectives** – what has to be achieved in order that each strand of the Argument is true (effectively, lower-level arguments)
- **Assurance Activities** – how the Assurance Objectives are met
- The **Evidence** – results of the Assurance Activities giving sufficient confidence that:
  - the Assurance Objectives have been met, and therefore
  - the Argument is true, and therefore
  - the Claim is valid!!
- "sufficient confidence" is defined by the Assurance Level (SAL) assigned to the system

EUROCONTROL

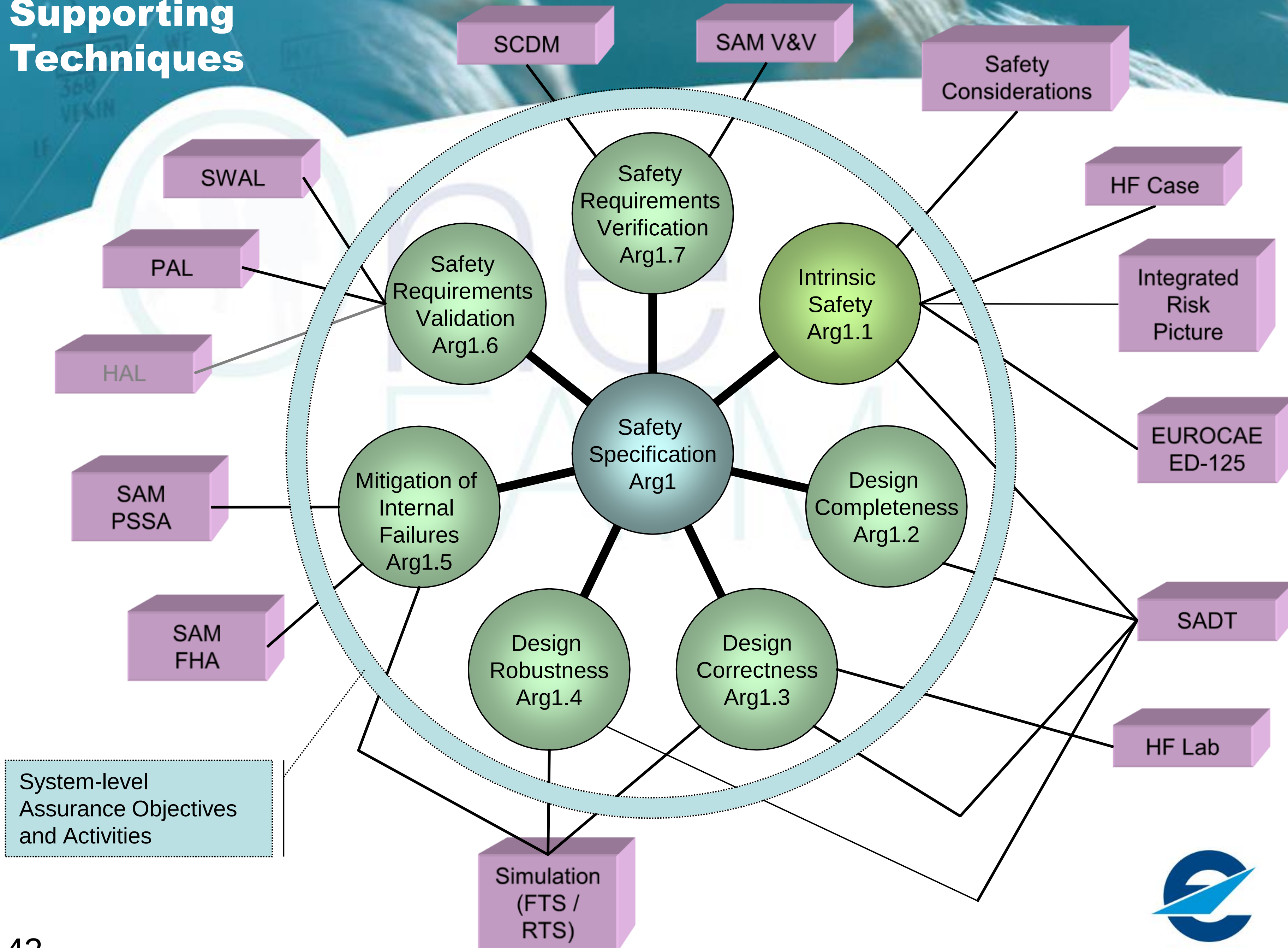
System Safety Assurance Objectives

Definition (i)	Design & Validation (ii)					
Arg1.1 Intrinsic Safety	**Arg1.2** Design Completeness	**Arg1.3** Design Correctness	**Arg1.4** Design Robustness	**Arg1.5** Mitigation of Internal Failures	**Arg1.6** SR Validation	**Arg1.7** SR Verification
i1 Identify initial safety issues and overall assurance objectives i2 Ensure that a Functional Model has been clearly described, which completely and correctly interprets the Concept of Operations i3 Ensure that the differences from existing operations have been described, in terms of, inter alia, the Functional Model, and shown to be compatible with the Safety Criteria i4 Ensure that the impact of the Concept on the operational environment (including interfaces with adjacent systems / airspace) has been assessed and shown to be compatible with the Safety Criteria i5 Ensure that the key (minimum) functionality and performance parameters have been defined and shown to be compatible with the Safety Criteria. i6 Set Safety Objectives for each internally-generated hazard such that the corresponding aggregate risk is within the specified Safety Criteria	ii1 Ensure that a Logical Model has been clearly described, which completely and correctly interprets the Concept of Operations and Functional Model. ii2 Ensure that everything necessary to achieve a safe implementation of the Concept – related to equipment, people, procedures and airspace design - has been specified (as function & performance safety requirements), for each element of the system ii3 Ensure that all safety requirements on, and assumptions about, external elements of the end-to-end system have been captured	ii4 Ensure that design (LM / FSRs etc) is coherent within itself ii5 Ensure that the system design operates correctly (and as per the Concept of Operations) in a **dynamic** sense, under all normal conditions etc ii6 Ensure that system design is capable of delivering (or maintaining) the required contribution to aviation risk reduction under normal conditions etc ii7 Ensure that the system design operates in a way that is compatible with the operation of adjacent airspace and external systems with which it interfaces / interacts ii8 Ensure that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets	ii9 Ensure that the system can react safely to all reasonably foreseeable abnormal conditions in its environment / adjacent systems, that are not covered under Arg1.5	ii10 Specify Safety Integrity Requirements and / or Assumptions for the causes of each hazard, such that the Safety Objectives (and/or Safety Criteria) are satisfied ii11 Capture all internal and external mitigations as either FSRs / SIRs or Assumptions ii12 Ensure that the system can actually operate safely under all degraded modes of operation identified above	ii13 Ensure that all aspects of the system design have been captured as either Safety Requirements (SRs) or Assumptions, as applicable ii14 Ensure that satisfaction of each SR can be demonstrated by direct means or (where applicable) indirectly through appropriate assurance processes ii15 Ensure that all SRs are capable of being satisfied in a typical implementation, in hardware, software, people and procedures. ii16 Ensure that all Assumptions are valid	ii17 Ensure all processes, tools, techniques etc used in Arg1.1 to 1.6 are adequate for the job ii18 Ensure that all staff involved in Arg1.1 to 1.6 are competent for the job

Examples of System Assurance Activities

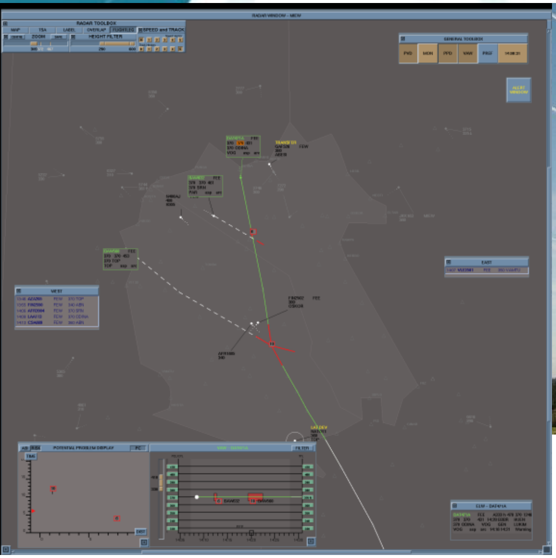
Definition Phase (i)		
Objective	**Activities**	**Guidance / Possible Tools and Techniques**
Arg1.1 - Intrinsic Safety		
i1 Identify initial safety issues and overall assurance objectives	a1. Identify the User Need a2. Show that CONOPS fully addresses User Need a3. Carry out Safety Considerations process and, if appropriate, Human Factors Fact Finding process a4. Determine appropriate Safety Criteria a5. Produce a Functional Model (FM), to fully interpret the CONOPS a6. Derive System Assurance Level (SAL) from FM view of the overall system a7. Derive SAL objectives for Definition and Design phases. a8. If appropriate, carry out Human Factors Issues Analysis. a9. Capture all unresolved safety issues from the Safety Considerations and HFIA as further **safety assurance objectives / activities** for the appropriate phases of the lifecycle.	See outline in section 4.3 of Part 1. For fuller description of **Safety Considerations** process, see **Error! Reference source not found.**. For **Human Factors Fact Finding** see the **Human Factors Case** outline at **Error! Reference source not found.**. General guidance on **Safety Criteria** is given in the SCDM **Error! Reference source not found.**. If it decided to use absolute safety criteria based on a **Risk Classification Scheme**, then see EUROCAE ED-125 **Error! Reference source not found.** for guidance. If it decided to use absolute safety criteria based on a **Target Level of Safety** TLS, then **IRP** may be able to provide a suitable quantitative TLS – see IRP outline at **Error! Reference source not found.** For some Operational Concepts – eg the introduction of automation of previously human processes – it may no be possible to capture all the aspects of the Concept at the level of abstraction of the FM. In these cases, it may be necessary to also produce a Logical Model (LM) at this stage. See section **Error! Reference source not found.** and **Error! Reference source not found.** See section **Error! Reference source not found.** and Table A.1 herein. See the Human Factors Issues Analysis (HFIA) in the **Human Factors Case** outline at **Error! Reference source not found.**. In general, Whether an **HFIA** is necessary is also matter of judgement depending on the SAL and on the complexity of the HF-specific aspects of the system. *[it is hoped to provide further, more specific guidance on these matters in due course]*.
i2 Ensure that a Functional Model has been clearly described, which completely and correctly interprets the Concept of Operations (CONOPS)	a10. Describe how the FM is intended to operate. a11. describe each of the Safety Functions that make up the FM a12. Show that the FM is internally coherent	For simpler, less critical systems, a straight forward paper description and analysis may well suffice. For more complex, more critical systems, use of structured analysis techniques and tools may be required – see **SADT** outline at **Error! Reference source not found.**
i3 Ensure that the differences from existing operations have been described, in terms of, inter alia, the Functional Model, and shown to be compatible with the Safety Criteria	a13. Determine and characterize existing operations. a14. If necessary, produce an FM for the existing operations a15. describe how the system under consideration changes the ATM operations a16. Explain how those changes are compatible with the satisfaction of the Safety Criteria	For most projects this is simply the operations relating to the system under consideration immediately prior to the proposed changes to, or introduction of, that system. For some projects, it may be appropriate to compare the new / modified system with a known, proven baseline that does not necessarily reflect the local pre-change situation – the introduction of ADS-B into previously Non-radar Airspace, as described in section 3.2 of Part 1, is a case in point

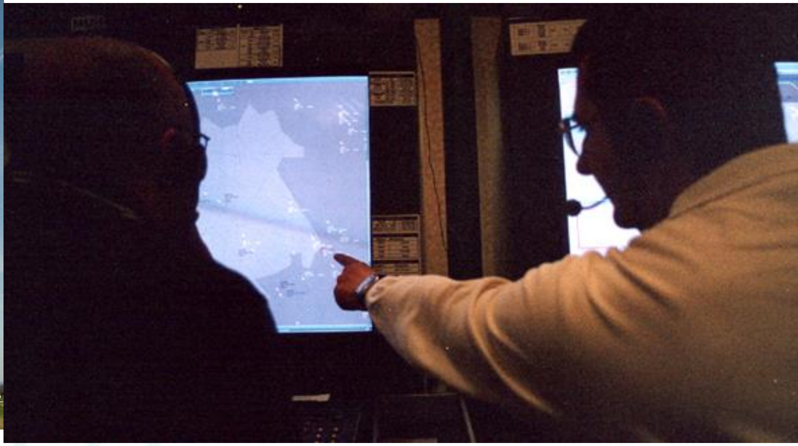
Supporting Techniques



EUROCONTROL

Questions ??





?

EUROCONTROL