A2COS
safety certification

AVIATION SAFETY & CERTIFICATION OF NEW OPERATIONS AND SYSTEMS

Stephen Bull
Ebeni Limited

Safety and Reliability Society Western Region – 24th March 2015

This presentation

- →Who am I?
- →What is ASCOS?
- →Who is involved?
- →Work packages
- →Outline Certification Approach
- →Case Studies
- →Refinement of Approach
- →Conclusions

Who am I?

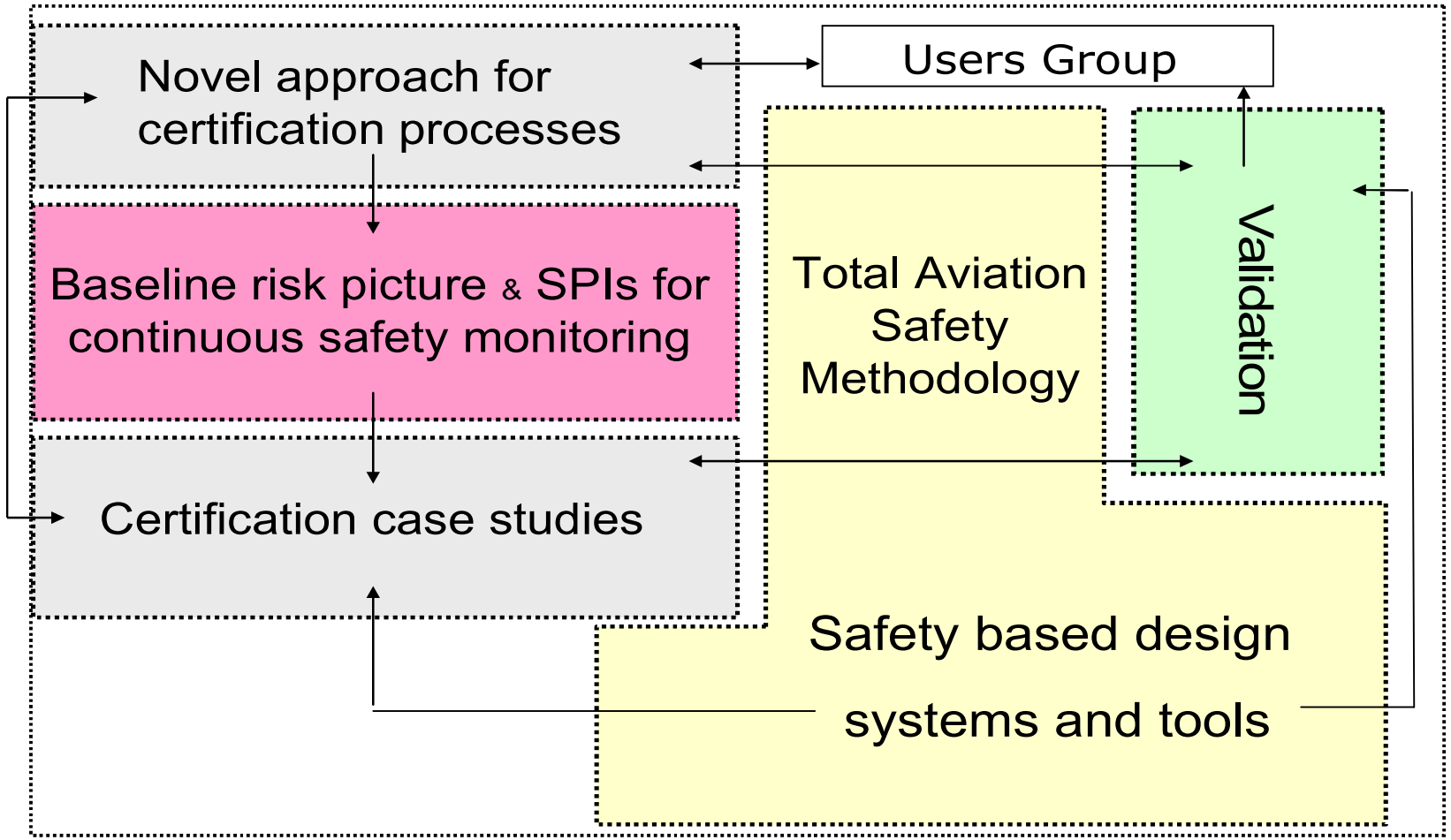
- Stephen Bull
- Senior Safety Engineer with Ebeni Limited
- 20 years' experience in safety related systems
  - aviation and rail sectors
  - software development
  - safety assurance and safety cases

What is ASCOS?

- *Goal: "To develop certification process adaptations, with supporting tools for safety based design and safety monitoring, so as to ease the introduction and certification of safety enhancements" in the European aviation industry*

- EU-funded under the Seventh Framework Programme
- Research project
- Started 1 July 2012
- Original duration 36 months
- Total cost ~ EUR 5m

Project Workpackages



Who is involved?

→ Industry partners:

NLR THALES APSYS RISK ENGINEERING CAAiV Isdefe ERTIFLYER

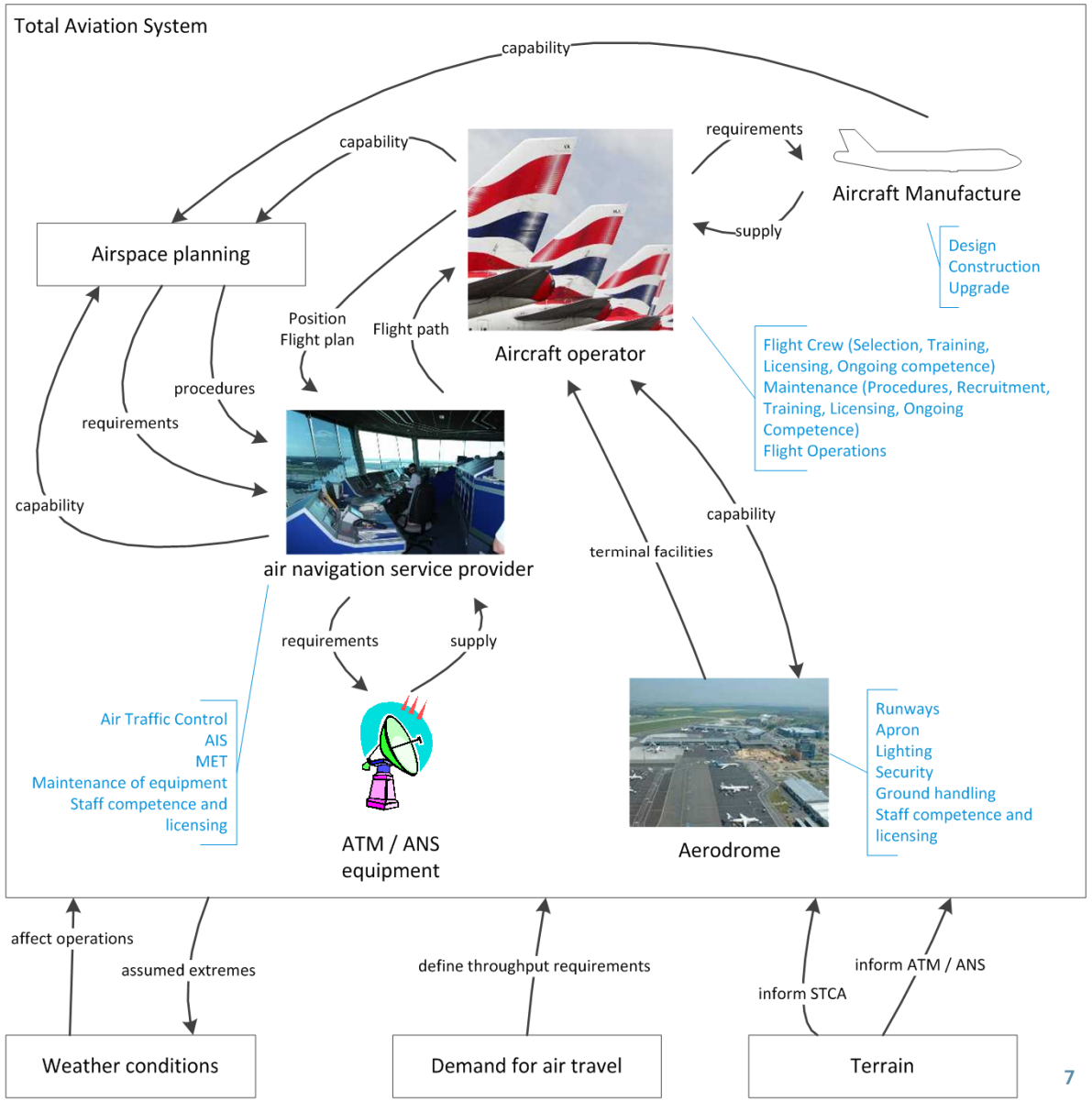
avanssa ebeni DEEPBLUE consulting&research JRC EUROPEAN COMMISSION TU Delft IL

→ Led by NLR (Dutch National Aerospace Laboratory)

→ User Group including:

- → CAAs (Dutch, Polish, UK), EASA EUROCAE
- → FAA FAST SESAR

Total Aviation System



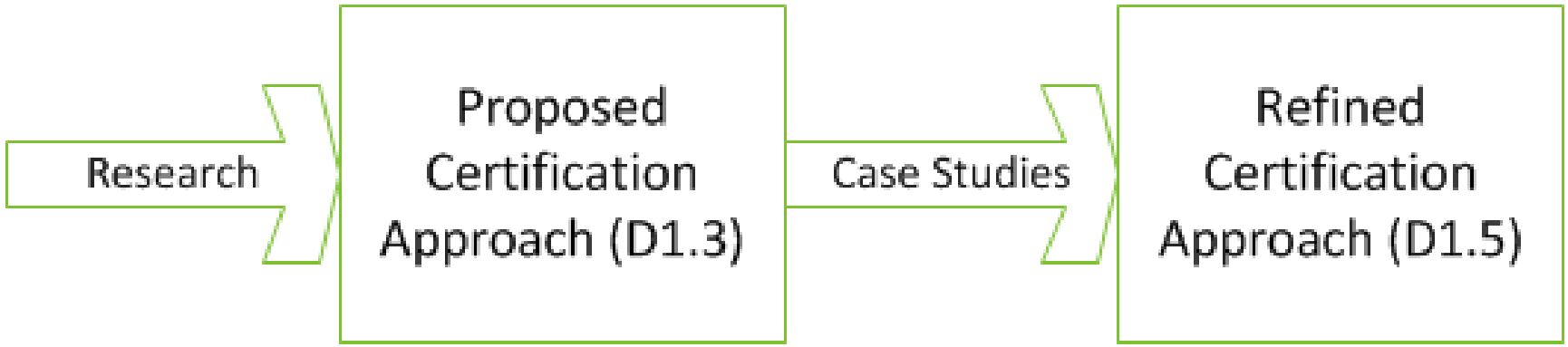
Problems with current processes

- Inter-domain issues
  - different safety standards
  - inconsistency of approach
  - ill-defined interfaces
  - lack of information exchange
- (Safety) *benefits* of change not fully considered
- Detailed specifications impede innovation
- Lack of understanding of regulations
- Concern over COTS certification

Certification approach - objective

- Develop an outline certification approach that could be used to cover the certification of changes in the Total Aviation System
- The new approach must offer improvements over the existing certification/approval processes in terms of
  - efficiency in cost and time
  - ability to analyse and demonstrate acceptable safety for new concepts and technologies
  - ability to analyse and consider the Total Aviation System rather than sub-elements in isolation
- Whilst not undermining the efficacy of existing process!

Project Status



Certification Approach Overview

- Eleven Step Approach Driven By Logical Argument
  - Covers Total Aviation System
  - Addresses whole lifecycle
- Retains proven elements of existing approaches
- Flexibility
  - for new technology
  - for cross-domain learning
- Manages interfaces between domains
- Overall argument needs an owner

Eleven Step Approach

- 1. Define the change
- 2. Define the certification argument (architecture)
- 3. Develop and agree certification plan
- 4. Specification
- 5. Design
- 6. Refinement of argument
- 7. Implementation
- 8. Transfer into operation – transition safety assessment
- 9. Define arrangements for continuous safety monitoring
- 10. Obtain initial operational certification
- 11. Ongoing monitoring and maintenance of certification

Case Studies

- Apply new approach on realistic examples
  - Only first steps of approach
  - Research only – not solution development
- Four studies
  - RPAS failure management
  - Automatic Aircraft Recovery System
  - Separate certification for on-ground de-icing
  - ATM / CNS systems for improved surveillance

Step 1: Define the Change

- Functional specification – not solution
- Impact across aviation system
- Applicable regulations
- Organisations involved

- Challenges
  - *too deep too quickly – incomplete definition*
  - *scoping the change*
    - *CS1: RPAS AFMS only part of change*
    - *CS3: what is the change?*

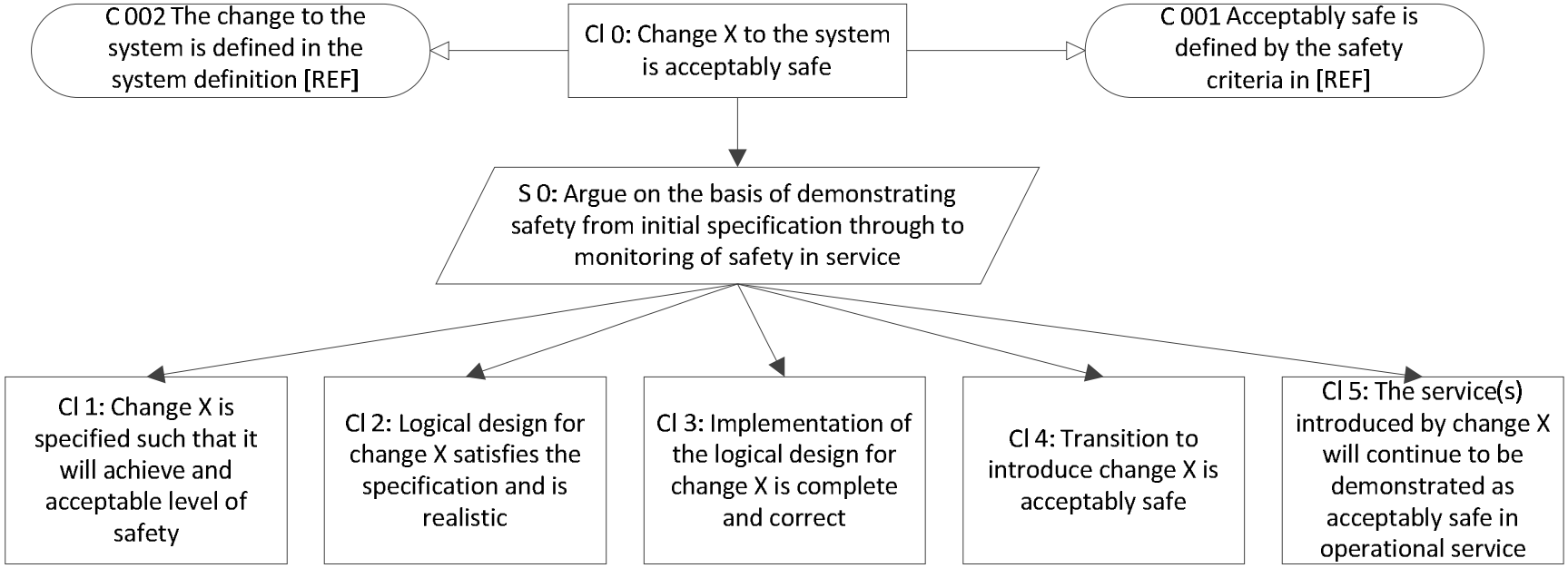
Step 2: Define the Argument

- Rationale for argument framework
- Example top level argument
- Argument modularisation
- Challenges

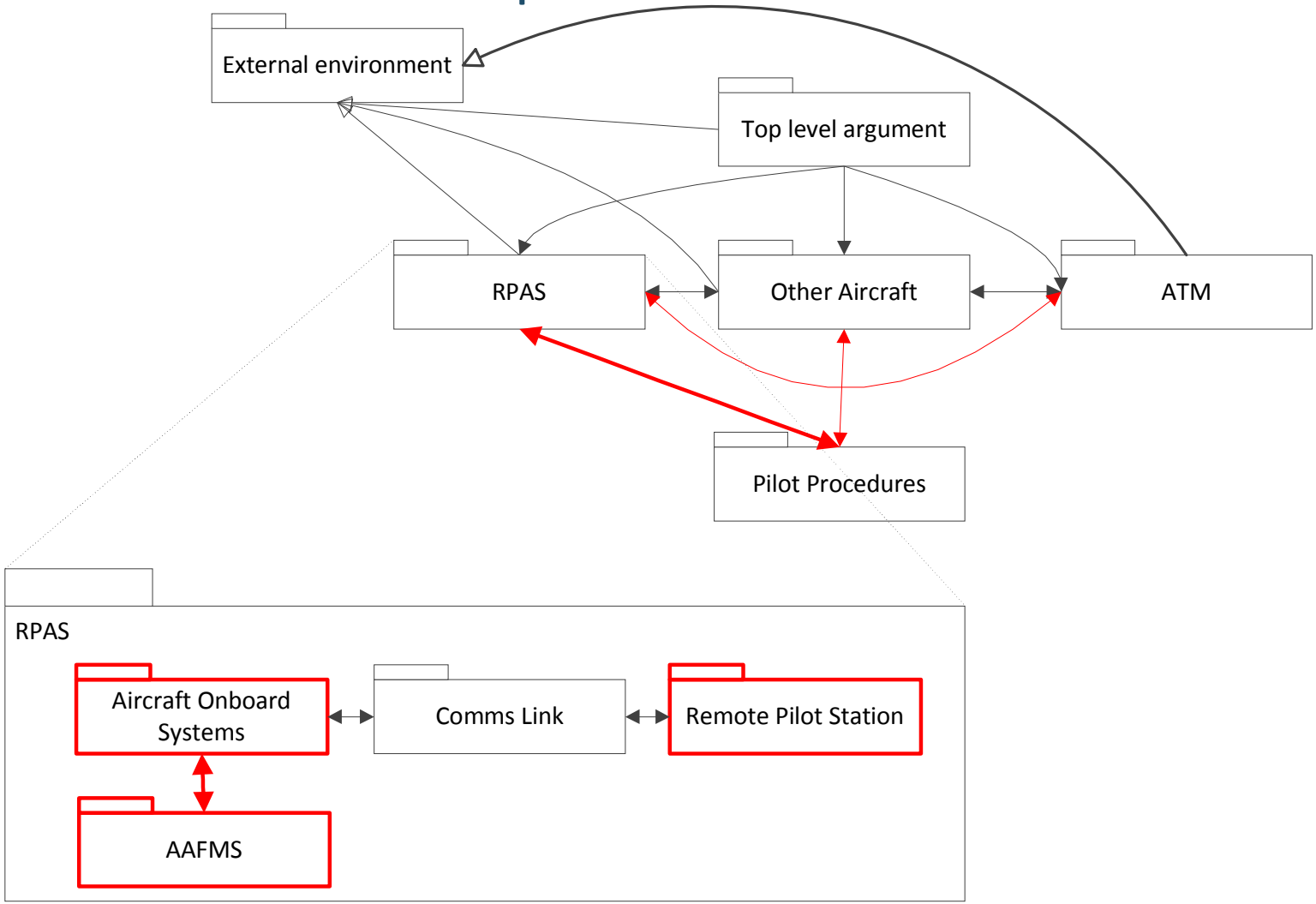
Rationale for Argument Framework

- Logical argument *framework* for *total system* certification
  - No universal panacea
  - Flexibility – e.g. for new technology
  - Adaptable to maturity of existing approach
- Integrate "arguments" made for each domain
  - Retain existing approaches within domains
  - Assess context of existing approaches
  - Identify, challenge and manage assumptions / gaps
    - Implicit and explicit
    - Arising from analysis and context
- Managing / owning the argument
  - Different parts "owned" by different organisations
  - Requires maintenance throughout lifecycle

Logical Argument



Modularisation - Example



Step 2: Define the Argument - Challenges

- Why do we need an argument?
  - Is “argument” a loaded term?
  - Can’t we just follow standards?
- Certification vs Acceptance
  - what is the goal of the argument?
- What is our safety target?
  - inconsistent between domains
  - possible help from other ASCOS Work Packages
- Who owns the argument?

Step 3: Develop and Agree the Certification Plan

- How will the change be “certified”?
- What standards / regulations?
- What evidence will be presented?
- When will evidence be presented?
- Who is involved?
  - applicants
  - competent authorities

- Challenges
  - *multiple authorities*
  - *different actors at different stages*
  - *inconsistent standards / requirements*

Steps 4-7: Safety of the Change - Overview

- Detailed specification, design and implementation
  - FHA, PSSA, SSA – or similar processes
  - ARP 4754 where appropriate
- Developing and supporting the argument
  - Using existing design and assessment processes where appropriate
  - Framework to adopt new processes where existing insufficient
- Identifying and managing interfaces between domains

Steps 4-7: Safety of the Change - Challenges

- Assessment process
  - Assessing adequacy of existing processes
  - Aligning the detailed argument to existing processes
  - How to adapt existing processes
- Inter-domain
  - Trading off safety between domains
  - Managing interfaces between domains
- Changing stakeholders
  - Different at each stage of argument
- Support from risk model

The remaining steps (introduction and operation)

- 1. Define the change
- 2. Define the certification argument (architecture)
- 3. Develop and agree certification plan
- 4. Specification
- 5. Design
- 6. Refinement of argument
- 7. Implementation
- 8. Transfer into operation – transition safety assessment
- 9. Define arrangements for continuous safety monitoring
- 10. Obtain initial operational certification
- 11. Ongoing monitoring and maintenance of certification

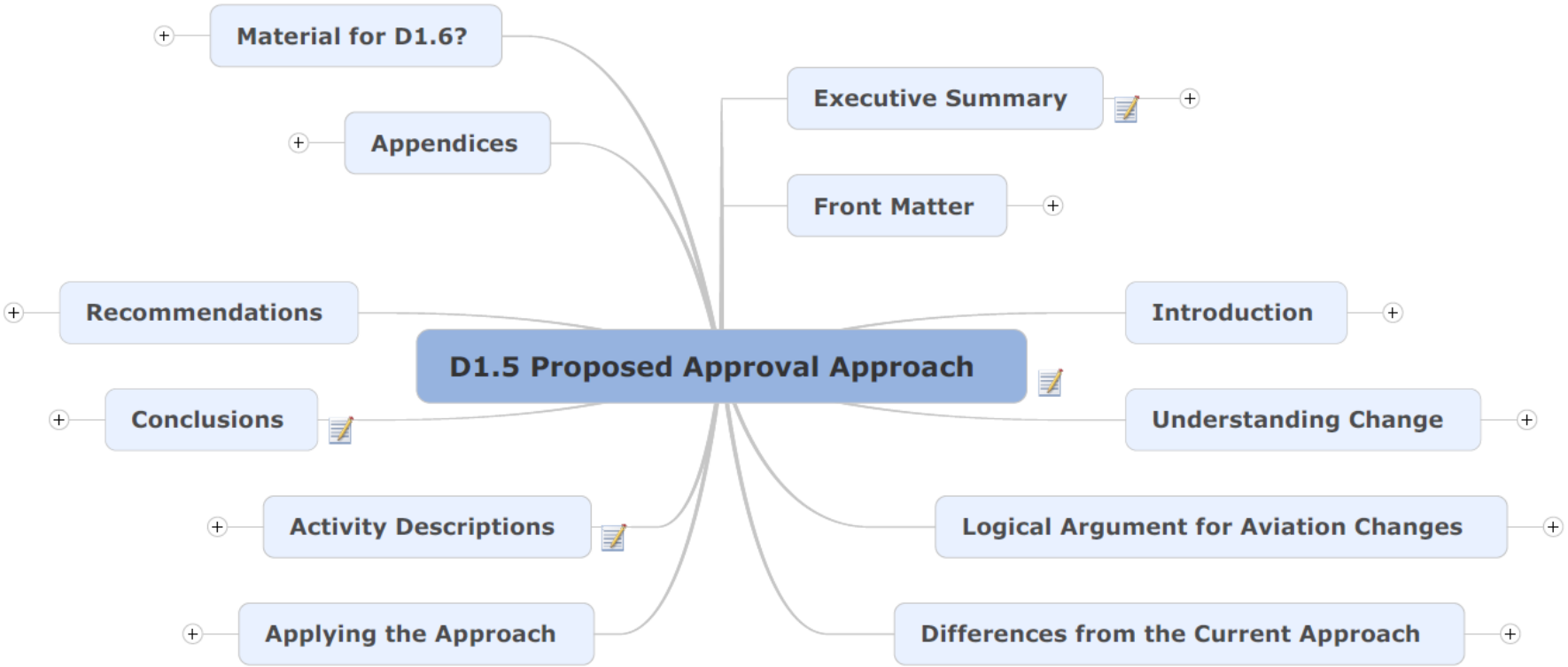
Summary of Challenges

- too deep too quickly (Step 1)
- scoping the change (Step 1)
- why do we need an argument? (Step 2)
- inconsistent safety targets (Step 2)
- who owns the argument? (Step 2)
- multiple authorities (Step 3)
- different stakeholders at different stages (Step 3)
- inconsistent standards / requirements (Step 3)
- assessing at the correct level of abstraction (Step 4-7)
- inconsistent approaches between domains (Step 4-7)
- terminology conflicts (general)
- insufficient guidance (general)

Refining the Approach

- Focus more on understanding and scoping change
  - before considering an argument
- Retain overall logical argument framework
  - explain how existing approaches have implied arguments
- Improved guidance, in particular:
  - tailoring argument to specific change
  - integrating existing standards / processes
  - how to capture interfaces between domains
  - certification planning
- Guidance on terminology
- Creation of templates to illustrate common scenarios

Report outline



Where are we currently?

- Difficult to certify change spanning Total Aviation System
- Well-established approaches within domains
- Main challenges are where change crosses domains
  - Different approaches
  - Different safety targets
- Logical argument framework
- Case studies have identified areas for improvement
- Now refining the approach for publication

Project website *http://www.ascos-project.eu*

- ASCOS coordinator:
  - Dr. Ir. Lennaert Speijker
  - NLR Air Transport Safety Institute
  - Email: speijker@nlr-atsi.nl
  - Phone : +31 88 511 3654

- Presenter
  - Stephen Bull
  - Ebeni Limited
  - Email: stephen.bull@ebeni.com
  - Phone: +44 1249 700555

A2COS

safety certification

NLR THALES APSYS RISK ENGINEERING CAAV Isdefe ERTIFLYER

avanssa ebeni DEEPBLUE consulting&research JRC EUROPEAN COMMISSION TU Delft IL