AVIATION SAFETY & CERTIFICATION OF NEW OPERATIONS AND SYSTEMS

Stephen Bull, Senior Safety Engineer
Ebeni Limited

Safety-critical Systems Symposium – 2\textsuperscript{nd} February 2016
What was ASCOS?

→ EU research project: July 2012 – October 2015
→ Tasked to streamline aviation approval processes
→ Cross-industry User Group
→ Industry Partners
Why was ASCOS needed?

→ Complex prescriptive processes
→ Innovation stifled
What we did

- Novel approach for approval processes
- Baseline risk picture & SPIs for continuous safety monitoring
- Certification case studies

→ Initial research
→ existing processes
→ accidents and incidents
→ other industries

→ Initial Proposed Method (D1.3)
→ Total Aviation Safety Methodology
→ Safety based design systems and tools

→ Application to Case Studies
→ Final Proposed Method (D1.5)

→ Validation
Principles for the Method
# Performance Based vs Compliance Based

<table>
<thead>
<tr>
<th><strong>Performance Based</strong></th>
<th><strong>Compliance based</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>high level</td>
<td>detailed</td>
</tr>
<tr>
<td>solution independent</td>
<td>solution-specific</td>
</tr>
<tr>
<td>goal based approach</td>
<td>“tick box”</td>
</tr>
</tbody>
</table>

| Support innovation    | Capture established rules |
|                       | Constrain interfaces     |

→ *Both approaches can be useful*
Overview of the ASCOS Method

1. Identify the need
2. Develop change definition
3. Develop approval path
4. Develop solution
5. Obtain approval
6. Operational Service

TAS Level Development

- Modularisation
- Domain Level Development
- Evaluation

from Develop Approval Path
to Obtain Approval
Safety Argument Approach

C 001 Acceptably safe is defined by the safety criteria in [REF]

C 002 The change to the system is defined in the system definition [REF]

S 0: Argue on the basis of demonstrating safety from initial specification through to monitoring of safety in service

Cl 0: Change X to the system is acceptably safe

Cl 1: Change X is specified such that it will achieve an acceptable level of safety

Cl 2: Logical design for change X satisfies the specification and is realistic

Cl 3: Implementation of the logical design for change X is complete and correct

Cl 4: Transition to introduce change X is acceptably safe

Cl 5: The service(s) introduced by change X will continue to be demonstrated as acceptably safe in operational service.

C 001 Acceptably safe is defined by the safety criteria in [REF]
Modular Arguments

RPAS

Top level argument

Other Aircraft

ATM

Pilot Procedures

Onboard Systems

Comms

Remote Pilot Station

Automated Failure Management

RPAS
Acceptable Level of Safety

→ Needs acceptance by all domains
→ Domains use different forms of target
  → absolute vs relative
→ Trade-off between domains
  → currently impractical
  → needs models which are
    → covering Total Aviation System
    → trusted
    → robust
An Argument Architect

- Top level argument
- Other Aircraft
- ATM
- RPAS
- Pilot Procedures
Further development

→ Definition of *domain / module boundaries*
→ *Who* should be the *argument architect*?
→ Document *current (implicit) arguments*
→ *Integrated* safety targets
→ *Sharing* safety information
Conclusions

→ Developed *framework* to streamline safety approval
  → *Existing approaches* are *reused* where appropriate
  → *Flexible* to allow *innovation*
→ *Modular safety argument* to integrate approval
  → Modules aligned to *domains*
  → Focus on *total aviation system*
  → Contracts to manage *interfaces* and dependencies
  → Overseen by *argument architect*
→ Critical to plan integrated *approval path* up front
→ Next step is trial application

→ *... read the full report* on the ASCOS website
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 7867 330843

This presentation has been realized partly with funding from the EC under the ASCOS Project (Grant No 314299). The support of ASCOS partners and Dr Michael Kyriakopoulos, EC Scientific Officer is greatly appreciated.