Improving European Aviation Safety Approvals

Stephen Bull[1]

Ebeni Limited

Corsham, UK

Abstract *The European aviation industry is experiencing wide-ranging change including introduction of new technologies and operational concepts, while also facing demands for higher levels of safety performance. Existing approaches to gaining approval are often perceived as a barrier to adopting innovation and change; they can also miss significant interactions between parts of the system. The EC-funded ASCOS Project has developed a method and supporting tools to address these challenges. The ASCOS Method uses modular safety arguments to provide a framework to integrate existing approval approaches while also providing the flexibility to adapt the approaches where necessary to enable the smooth approval of advances in aviation technology.*

1 Background

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance all call for the adaptation of existing approval processes.

The increasing amount of technological innovation within the industry challenges existing prescriptive regulations used in aircraft certification. These regulations are an established and effective way of capturing lessons from past experience to ensure that future implementations learn from these lessons, thus delivering safer operations. However, innovative solutions often cannot comply with such prescriptive regulations, making it difficult to demonstrate that solutions meet industry safety requirements. There is therefore a move towards performance based regulation where the applicant for approval must demonstrate compliance

[1] Stephen Bull is a senior safety engineer at Ebeni. He can be contacted at stephen.bull@ebeni.com

with a level of safety, but where there is freedom on the way in which that level of safety is achieved.

The shortcomings of existing processes are illustrated in the FAA Commercial Airplane Certification Process Study (FAA 2002), which concluded that there was no reliable process to ensure that assumptions made during solution development and assessment are valid with respect to operations and maintenance activities and, furthermore, to ensure that human operators are aware of these assumptions when developing their operations and maintenance procedures. It also became clear during the study that aircraft certification standards may not reflect the actual operating environment. Other studies have reached similar conclusions.

2 The ASCOS Project

In reaction to the drivers described above, the EU ASCOS[1] Project was established to develop a novel and innovative approach towards approval in order to ease the efficient and safe introduction of safety enhancement systems and operations. This novel approach was required:

- to be more flexible with regard to the introduction of new products and operations;
- to be more efficient, in terms of cost and time, than the current certification processes;
- to consider the impact on safety of all elements of the aviation system and the entire system life-cycle in a complete and integrated way.

Development of this novel approach was supported by safety-driven design methods and tools to ease the approval process. The project has followed a total system approach, dealing with all aviation system elements (including the human element) in an integrated way over the complete life-cycle.

The ASCOS programme was structured into six main work packages (WPs):

- WP1: Certification Process – Development of safety based certification process adaptations based on analysis of existing certification and evaluation of possible new approaches
- WP2: Continuous Safety Monitoring – Development of a methodology and supporting tools for continuous safety monitoring, using a baseline risk picture for all parts of the Total Aviation System (TAS)
- WP3: Safety Risk Management – Development of a total aviation system safety assessment methodology for handling of current, emerging and future risks

[1] Aviation Safety and Certification of new Operations and Systems

- WP4: Certification Case Studies – Application of the new certification approach to selected example case studies
- WP5: Validation – Validation of the new certification approach, supporting methods and tools
- WP6: Dissemination and Exploitation – Dissemination to ensure that results are correctly understood and exploited to the maximum extent.

There was also a seventh work package for project management. The relationships between these work packages are depicted in Figure 1.

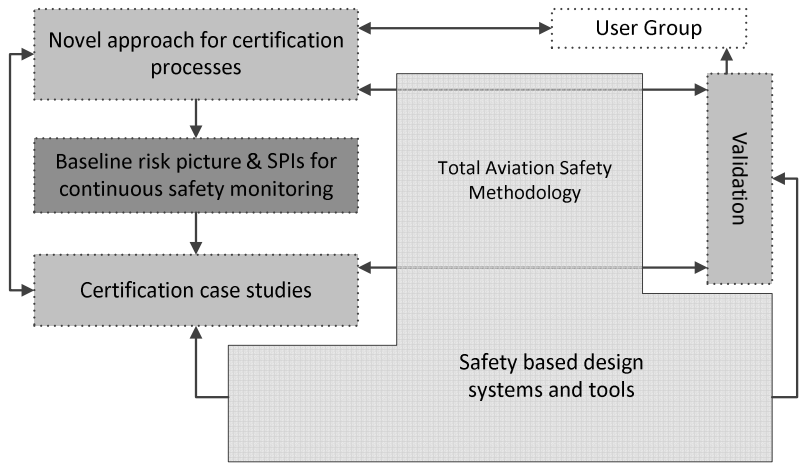

Fig. 1. Relationships between ASCOS work packages[1]

The final reports from the work packages are listed at the end of this paper and are available for download from the ASCOS Public Website[2].

The three year programme was an EC-funded partnership with participants[3] drawn from the aviation industry, including national Civil Aviation Authorities (CAAs), research organisations and consultancies. Ebeni led the effort to develop the novel approach for certification processes. A User Group was constituted to provide input from across the aviation industry.

This paper focuses on the development of adaptations to the existing certification and approval processes (i.e. WP1).

[1] Arrows indicate the flow of information between work packages.

[2] https://www.ascos-project.eu/

[3] A full list of participants can be found on the project website.

3 Key Concepts

The issue of concepts and terminology posed a real challenge, especially where the same term is interpreted differently across the aviation industry.

This section introduces some key concepts on which the ASCOS Method was built.

- The term **certification** is widely used in the aviation industry to describe the process of demonstrating that a physical item, or an organisation, meets a defined set of requirements and can therefore be issued a certificate to confirm this compliance. For example, certificates are granted for aircraft, air operators, providers of air traffic services. The ASCOS Method, although originally conceived as an adaptation of certification processes, is intended be applicable more widely, to any change requiring approval.
- **Approval** is a broader term than certification, covering the process where the relevant approver (usually a designated competent authority) gives approval for a change to the Total Aviation System (TAS). For example, approval may be granted to change the way in which an air traffic service is provided at a particular aerodrome.
- The **Total Aviation System (TAS)** refers to all elements of the system which provides an aviation service, including concepts, equipment, people and processes.
- The TAS is subdivided into **domains**; although domains are not formally defined in the method, they can be aligned to the structure of the applicable regulations under which approval will be granted.
- A **change** is any alteration to the TAS, beyond intended operational use or maintenance. Changes range in scope from upgrade of existing equipment items through to introduction of a new operational concept. Changes need approval before they are introduced into operational service; approval is usually given by the relevant authority (e.g. either the European Aviation Safety Agency (EASA) or the relevant national CAA).
- The concept of a modular **safety argument** will be familiar to most readers: in this context it is defined as a connected series of statements, with supporting evidence, used to persuade the reader of the correctness of an overall claim about the safety of a change. The argument is divided into **modules** (which may be aligned to the domains of the TAS) and the dependencies between modules are captured in **assurance contracts**.

4 Developing the Method

Initial research was undertaken to survey the state of certification processes in the aviation industry and to identify options for change (see section 4.1), published as

(ASCOS 2013a). As a result, an initial proposal for the ASCOS method was developed (ASCOS 2013b) (see section 4.2). This method was then applied using four case studies (see section 4.3) and evaluated through validation workshops (see section 4.4); the findings are summarised in section 4.5. The final version ASCOS Method (ASCOS 2015a) was then developed, based on these findings. Key features of the method are presented in section 5.

4.1 Options for Change

Initial research (ASCOS 2013a) into existing approaches and opportunities for improvement identified a number of principles to include in the ASCOS Method. These can be summarised as follows:

- taking a Total Aviation System (TAS) approach
    - provide a generic certification framework covering the TAS and the whole system lifecycle
    - standardise language across all domains
    - harmonise approaches between domains where appropriate
    - consider the balance between product and organization certification
    - promote flexibility within each domain to allow introduction of new technologies or procedures
- development of current processes
    - keep the existing approach where possible, minimising unnecessary change and recognising the good approaches already in place
    - simplify certification processes, where there are demonstrable benefits and no loss of confidence in the assurance of safety
    - learn lessons from other domains where this gives improvement
- fully considering interfaces between domains and organisations
    - provide rigorous management of interfaces, between domains and between the TAS and its environment, to ensure that all key safety issues are properly addressed and not lost at interfaces
    - establish a process for ensuring validity of assumptions, in particular with respect to operations and maintenance activities
- address known problems with existing approaches
    - reinforce existing techniques where they are appropriate but not consistently applied
    - provide a mechanism for identification and resolution of further bottlenecks and shortcomings
- specific issues
    - take more explicit account of electronic hardware in the proposed approach

- consider that less experience is gained by flight crew when more automation is used

The research also identified eight options for change. Evaluation of these options focused on identifying those with the greatest potential for safety and cost benefit, although it also considered other criteria. The four options chosen for further development were:

- Change between performance based and compliance based
- Use of Proof of Concept approach
- Enforce existing rules and improve existing processes
- Cross-domain fertilisation

The overriding consideration when designing the ASCOS Method was the need to develop a method which accommodates and integrates existing approaches while allowing for extension and adaptation of these approaches where necessary. The details of the method described in D1.5 (ASCOS 2015a) show how the principles and chosen options have been addressed.

4.2 An Eleven Step Process using Logical Argument

It was apparent early in the project that there is no single approval approach universally applied within the TAS, and that the role of ASCOS was to develop a framework which allows existing approaches to be integrated, and adapted where this is either necessary or beneficial.

The need to integrate multiple sources of information and evidence into what is effectively a single claim about safety led the team towards the concept of a safety argument. We also proposed to modularise the argument (see, for example, Fenn et al. 2007), aligning the modules to the boundaries of domains and organisational responsibility, with assurance contracts established between the modules to formally define and manage dependencies.

The use of logical argument was supported by an eleven step process as follows:

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

Some written guidance was produced for each step, but the case studies (see below) applying the method were also supported by the team that had developed the method. Further written guidance was produced when the method was updated in light of this experience.

The report (ASCOS 2013b) describing this initial version of the method is available on the ASCOS public website. This initial description of the ASCOS Method went some way towards showing how concerns and options identified in the early work are addressed by the method.

4.3 Case Studies

When the eleven stage method had been developed, it was applied to the following four case studies intended to examine how it could be applied to realistic approval challenges:

1. Remotely Piloted Aircraft System (RPAS) failure management
2. Automatic Aircraft Recovery System (AARS)
3. Separate certification for on-ground de-icing
4. ATM / CNS[1] systems for improved surveillance

Each case study was developed over the period of a year (2014) by teams drawn from organisations participating in the ASCOS Programme. Each case study attempted to apply the ASCOS Method by developing a logical argument and approval plan, each with varying degrees of success.

As the case studies were desk top exercises, with limited time and effort available to them, they were only able to apply the early stages of the method. However, they produced valuable feedback which was used to improve the method.

A report on the case studies is published as (ASCOS 2015e).

4.4 Validation

The case studies were complemented by familiarization and validation workshops where the interim results of the ASCOS Programme were presented to the User Group: their feedback was elicited with the help of a questionnaire, completion of which was followed by a focus group meeting involving experts representing different aviation and certification domains. One of the validation exercises focussed

[1] Communication, Navigation and Surveillance

on the ASCOS Method itself (as initially presented as an eleven step method); the other exercises considered supporting tools.

A report on the validation activities is published as (ASCOS 2015f).

4.5 Recommendations

The case studies and validation exercises made the following recommendations for the improvement of the ASCOS Method:

- define the roles, responsibilities and team structures required to use the ASCOS Method
- use existing, and consistent, terminology where possible, and make this understandable to as wide a range of users as possible
- align the subdivision of the TAS into domains to the subdivisions contained within the EASA regulation structure
- refer to relevant assessment methods, in particular focussing on human factors and organisational assessment
- explain how to determine whether the ASCOS Method is applicable to a particular change
- explain how the ASCOS Method aligns to existing certification practice
- provide guidance on the definition of a change and its boundaries
- provide extensive guidance on the development of logical arguments
- provide guidance on how stakeholders should work together to apply the method, in particular where multiple domains with different approval regimes are involved
- provide guidance on how to develop a safety target which is unified across the TAS

Note: the recommendations have been simplified and combined for the purpose of presentation here. The full list of recommendations, including recommendations made to the EC and EASA is presented in a publicly available report (ASCOS 2015e).

5 The ASCOS Method

5.1 Introduction

The final ASCOS Method was developed (from the interim version) using the recommendations and experience from the case studies and validation workshops. The method is based on modular safety arguments and presents a framework of activities to be used to:

- understand and evaluate the change to the TAS
- identify the affected domains and stakeholders
- decide the path to be taken to gain approval (the approval path)
- agree the approval path with approvers via an approval plan containing an outline safety argument
- develop the modules of the safety argument in parallel with the development of the solution until the safety argument is ready to be presented for approval.

The method is illustrated in Figure 2, with the detail within the 'Develop solution' step illustrated in Figure 3. The detailed explanation of the method is published as ASCOS Deliverable D1.5 (ASCOS 2015a).

The ASCOS Method recognises that changes vary from simple equipment replacement to introduction of new complex concepts involving significant development, both of concepts and products. It also promotes the establishment of a TAS Engineering and Safety Group (TESG) for complex changes, responsible for co-ordinating the engineering and safety activities of all organisations involved in such changes and taking the role of argument architect.

The following sections present the key features of the ASCOS Method.

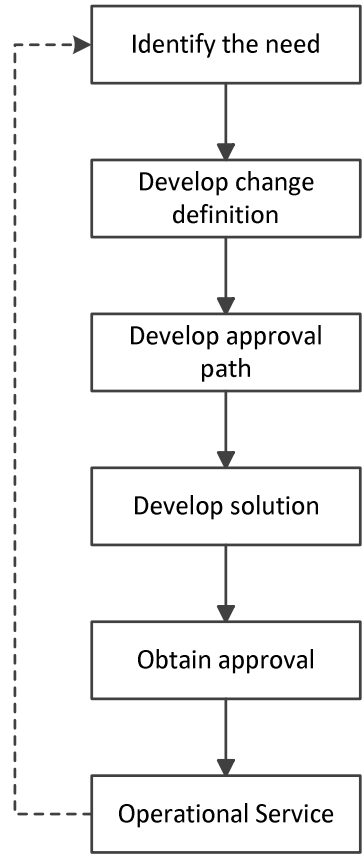

Fig. 2. Overall View of the ASCOS Method[1]

[1] The dashed line shows that experience from operational service may lead to identification of the need for further changes.

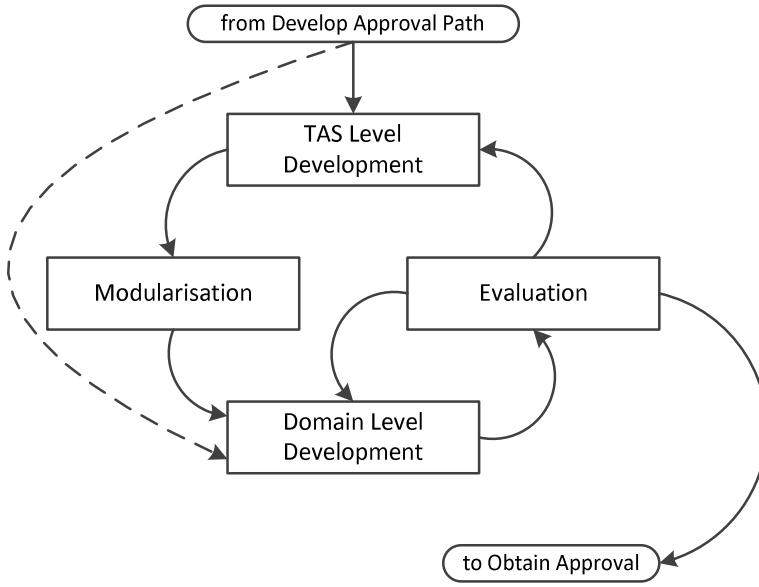

Fig. 3. Cyclic development of solution and safety argument[1]

5.2 Modular Safety Arguments

The concept of Modular Safety Arguments will be familiar to many readers, although such arguments are not used in all areas of the civil aviation industry. It is worth noting that even where the safety argument is not explicitly documented, any application for approval will rely on an underlying implicit argument, which may be embedded in the regulations against which the application is made. See (Holloway 2015) for a further discussion of implicit arguments underpinning standards. We also chose to express these arguments using Goal Structuring Notation (GSN) (GSN 2011), although this is not mandated and there are alternative ways to express safety arguments.

We proposed a top level argument (see Figure 4), based on a commonly used approach within Air Traffic Management (ATM) (EUROCONTROL 2010), with a top level claim that the change being made to the TAS is acceptably safe. The strategy chosen is to align the argument to stages of the lifecycle, including both

[1] Development may follow the dashed line if no further development of the solution at TAS level is required.

the transition of introducing the change and the continued monitoring of safety performance in service.

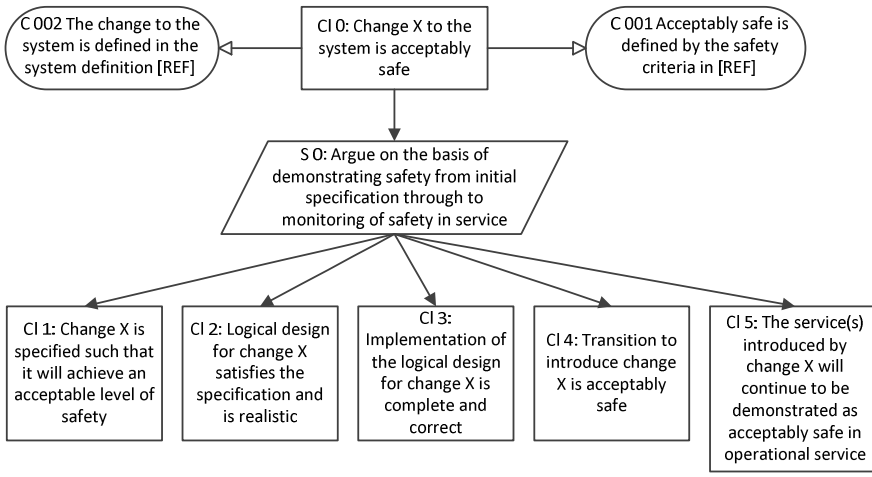

Fig. 4. Generic Top Level Argument

We also proposed to modularise the argument (see, for example, Fenn et al. 2007), aligning the modules to the boundaries of domains and organisational responsibility, with assurance contracts established between the modules to formally define and manage dependencies.

This argument is then decomposed in the usual way, with emphasis on introducing evidence from existing approaches and specifications as soon as possible. This minimises the amount of argument development needed, especially where the existing approaches are adequate. The main areas of argument development envisaged are:

- where the proposed change introduces innovation beyond the scope of existing standards
- where it is necessary to ensure that interfaces between parts of the system are fully addressed.

Modular safety arguments are not a universal panacea; however the concept provides a framework within which the applicant(s) can demonstrate to relevant approvers that any proposed change with the TAS achieves the defined acceptable level of safety. The framework provides a structure within which existing approaches can be evaluated and applied (and augmented where necessary) while also integrating them across the whole TAS.

5.3 Acceptable Level of Safety

The ASCOS Method focuses on demonstrating that the change delivers an acceptable level of safety across the TAS. In other words, the level of safety after the change must be acceptable to all competent authorities who will need to approve the change. *Note: this does not necessarily mean that an improvement in safety must be demonstrated.*

It is therefore necessary to determine appropriate safety targets in each domain affected by the change and demonstrate that each of these is met. Such criteria may be either absolute (specific safety objectives and integrity requirements based on apportionment of a safety target) or relative (comparison of the risk prior to the change against the predicted risk following the change). In the civil aircraft domain, the existence of the target for a catastrophic failure of 10^{-9} per flight hour makes it much easier to apportion absolute targets, whereas the absence of (and difficulty of defining and agreeing) similar absolute targets in other domains means that relative targets are often used.

As a result, each module of the safety argument will need to demonstrate that the change achieves the acceptable level of safety applicable in the domain for which the module is making the safety argument.

It should be noted that a change which increases safety risk in one domain is usually difficult or impractical to justify, even when it significantly decreases safety risk overall. Such a justification would need to be based on robust quantification across all domains which demonstrates a significant overall decrease of safety risk. Production of such a robust quantification is made more difficult by the fact that different domains use different types of targets (often with different units), making it difficult to create valid comparisons between domains. A similar assessment would also be needed in the event of a change with differing impacts on different sovereign states.

5.4 Developing and Agreeing an Approval Path

The overall intention of the ASCOS Method is to gain approval for a change to the Total Aviation System (TAS). Approval is granted by the approver on the basis of a safety argument (supported by evidence) justifying that the change will be acceptably safe.

The ASCOS Method can be viewed as establishing an approval path which, where possible, is based on existing approaches. For some changes, the approval path can be based entirely on existing approaches and appeal to the existing (possibly implicit) safety argument. An example of such a change might be the introduction of an upgraded equipment item on board an aircraft, where the new item has the same fit, form and function as the existing item. This could be visualised as a straight, already-established path, as shown in Figure 5.

Fig. 5. Approval path using existing approaches

For other changes, established approaches will provide the majority of the evidence needed, but with some gaps. In this case, the approval path may be established by developing approaches which cover the novel solution. These approaches must be developed in a way which takes account of the interface between the novel parts of the solution and the rest of the solution, to make sure that these are fully considered and integrated. The development of these additional approaches provides the missing part (see Figure 6) of the path to solution. This must then be supported by a safety argument which demonstrates that the combination of existing and new approaches fully addresses the change and that the resultant solution is acceptably safe.

Fig. 6. New approaches developed to complete the approval path

The analogy can be extended to approval paths which improve the efficiency of existing paths, or which may need to be developed from scratch (Figures 7 and 8).

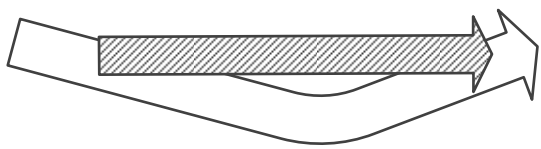

Fig. 7. New approaches developed to provide more efficient approval path

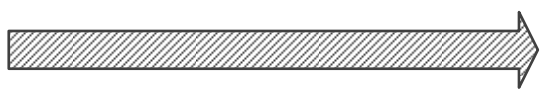

Fig. 8. Development of entirely new approval path

Complex or large changes may involve a combination of the above, as illustrated in Figure 9. Note that in these cases it is important to review the approaches against each other to ensure that the overall approach remains consistent in achieving the overall objective of a safe change to the TAS.

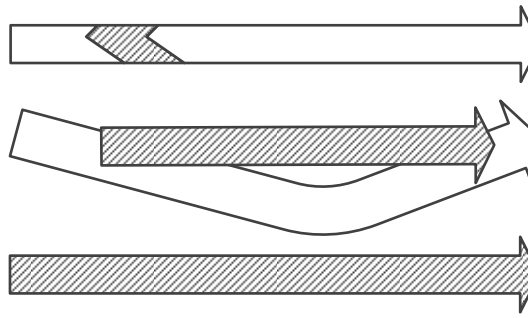

Fig. 9. Different approval paths for different parts of the system

In each case (with the possible exception of where the path exactly follows existing approaches), a safety argument is needed to demonstrate that the change achieves the defined acceptable level of safety. However, the scope of the argument required depends on the degree of novelty involved and on the degree to which the change spans multiple domains of the TAS.

The approval path should be documented in an approval plan. It is very strongly recommended that the safety argument and the proposed supporting evidence should be agreed between applicant and approver. If this agreement is not achieved early in the development, there is a significant risk that the safety argument and evidence produced by the applicant will not be acceptable to the approver. The applicant may then need to incur significant extra effort (and significant delay) in order to produce the evidence required. At worst, the approver may be completely unable to accept the proposed change.

5.4.1 Evaluating Existing Approaches

Great care is needed when evaluating existing approaches to determine whether they need adaptation or enhancement for the specific change. This is especially true where approaches or standards are being applied outside their usual context, or to novel solutions. It is necessary to ensure that the underlying assumptions remain valid; however, this can also be a very difficult task where assumptions are not clearly identified.

This can be illustrated with an example from the adoption of composite materials in airframes. Certification Specifications (CSs) specify the requirements which must be met in order to obtain a Type Certificate for an aircraft; however they are generally not specific to a particular type of material. As metallic structures have been the norm in airframes for many years, the CSs often (implicitly) assume a metal airframe. Some of these assumptions are evident, e.g. references to corrosion; others are less obvious. For example, the mechanisms for growth of cracks in metal structures mean that some cracks can be tolerated, as long as they are detected and monitored. However, damage growth in composites can be rapid, un-

predictable and not readily detectable, meaning that a very different approach is needed for composites compared with metal structures.

This is an example of where review of context and assumptions has led to revision of the specification on which certification (and subsequently approval) is based and is addressed in EASA Guidance Material (EASA 2010). Further details can be found in (JAM 2014).

5.5 Modularisation

The ASCOS Method addresses the issue of interfaces within the TAS by introducing the concept of dividing the argument into modules aligned to domains of the TAS and organisational responsibilities. Assurance contracts are established between modules to define and manage dependencies between modules.

This approach has the advantages of:

- making the overall safety argument easier to visualise and understand
- allowing modules to be developed separately from one another in confidence that the final result will be consistent and correct
- partitioning the safety argument such that each approver needs only:
  - to consider specified modules of the safety argument
  - to be assured that the assurance contracts at the boundary of those modules are correctly implemented

Modularisation also allows assumptions and dependencies which might otherwise be lost at the interface between domains to be formally agreed and documented – although this is not sufficient on its own: affected parties must also fully understand their responsibilities and commit to meeting them. This is particularly important given that such interface issues are a key concern within the aviation industry: see for example (AAIB 2015). Further general discussion of modularisation techniques can be found in (Fenn et al 2007).

Modularisation in the ASCOS Method principally involves:

- decomposing the TAS level claims into a complete set of supporting claims spread across each of the domains of the TAS
- determining the assurance contracts between the domains which allow the claims to be made in each of the domains
- specifying the context within which each claim must be demonstrated is completely captured to ensure that the evidence delivered is valid – this includes ensuring that the relevant context is specified within the assurance contracts

Effective management of modularised arguments depends on the argument architect role described below.

5.6 The Argument Architect

As described above, modularisation allows subdivision of the argument into modules, with assurance contracts between these modules allowing them to be developed separately from one another in confidence that the final result will be a consistent and correct overall argument. However, this also introduces a significant risk of divergence between the modules in ways which were not envisaged when the modules were created. It is therefore necessary to ensure that the argument is properly maintained and integrated throughout the development of the change.

When engineering complex systems, the role of system architect is responsible for the design of the overall system; this includes ensuring the integration of the resultant modules. The ASCOS Method gives the argument architect the similar role of designing and maintaining the safety argument, which includes ensuring that the argument modules are correctly bounded and interfaced to other modules throughout the development.

When considering the number of organisations involved in the TAS and their disparate roles, it is often not easy to identify who should be the argument architect. This in part explains why a key concern within the industry is the inadequacy of the management of interfaces between domains; sometimes integration is supervised by the approver or even ignored altogether.

ASCOS proposes (ASCOS 2015c) that any complex development should be co-ordinated by a TAS Engineering and Safety Group (TESG); the TESG would be responsible for co-ordinating all the engineering and safety activities involved in the development of the change. The TESG would therefore play the role of argument architect for changes involving multiple organisations.

5.7 Developing the Safety Argument

The top level safety argument (see Figure 4) needs to be decomposed into subclaims until a level is reached where the claims can be directly supported by evidence.

Within the ASCOS Method, the safety argument is mainly being used to make the link between:

- the high level safety targets embodied in the regulations
- the evidence (to be) produced

The aim is for this evidence to be produced by following existing processes wherever possible and a part of the process of developing the safety argument is a search for links between the safety targets and the evidence produced by existing processes.

The development of the argument should be specific about the evidence required and why it is required; this supports the exercise of reviewing the argument to determine whether the argument claims are in turn satisfied by that evidence.

Where development of the argument leads to requirements for additional evidence which would not be produced by following the usual processes within the domain, this highlights the fact that additional approaches need to be defined and followed.

Where the evidence produced by existing approaches (e.g. standards, AMCs) is sufficient to support the claim, the safety argument should only be developed down to the execution of that approach, along with justification that the context assumed by the approach matches the context required by the safety argument.

Where new or adapted approaches are developed, it may be necessary to develop the safety argument in more detail in order to develop and justify new approaches to generate the required evidence. Especially where new approaches are developed, the safety argument should be specific about the evidence required and why it is required; this supports the exercise of reviewing the safety argument to determine whether its claims are in turn satisfied by that evidence.

5.8 Performance Based or Compliance Based?

Approaches to approval are often characterised as either performance based or compliance based. This terminology can be used to distinguish between:

- requirements or targets which are relatively high level and solution independent (performance based) and
- requirements which are expressed as a detailed set of constraints often assuming a particular solution

The terminology can also be used to distinguish between:

- the goal based approach often used in ATM and
- the certification based approach often used in the aircraft domain

Although there is overlap between these two different ways of viewing the approaches, it is useful to bear both views in mind.

One concern driving the ASCOS Project is that parts of the aviation industry have historically taken a compliance based approach to approval and that this approach stifles innovation because specifications based on historical solutions can be difficult to apply to novel solutions. The performance based approach has been suggested as a way of allowing developers the freedom to innovate and therefore develop optimal solutions. In practice most approvals use a mixture of approaches – for example, the main requirement in the Certification Specification (CS) for

Large Aircraft (EASA 2015) relating to failure analysis (CS25.1309) is goal based, whereas the rest of the CS largely contains prescriptive requirements.

The ASCOS Method allows a goal based approach using high level, solution independent targets to support the development and assessment of innovative solutions, while also allowing more detailed requirements to be used to ensure consistent application of established solutions. Prescriptive requirements (a compliance based approach) are also useful to constrain interfaces or express well established rules, especially where these relate to interfaces with parts of the TAS unaffected by a change.

5.9 Who and When

Table 1 illustrates the roles involved in applying the steps of the ASCOS Method.

This introduces the concept of a change leader, which is the organisation with the primary motivation to make the change to the TAS happen. This organisation will lead the application of the ASCOS Method with support from other organisations. The change leader is responsible for developing the overall plan for approval of the change: through the TESG the change leader will work with the other stakeholders to ensure that the change is developed in a way which is coherent across the whole TAS. The change leader is likely to be the organisation introducing the change into service and therefore likely to also be (one of) the applicant(s).

The approver is the organisation responsible for approving the change. A change may involve multiple approvers, or multiple disciplines within a single approver organisation. Often the approver will be an authority such as EASA or the relevant national Civil Aviation Authority (CAA).

Table 1. Involvement within the ASCOS Method

	Change Leader (supported by TESG)	***Applicant***	***Approver***	***Argument architect***	***Manufacturer***	***Other affected organisations***
Identify the need	The need for a change may be identified by one or more parties across industry: the type of need will then drive which organisation(s) become change leader.					
Develop change definition	Lead definition of change at TAS level	Support development of change definition	Support change definition	*None*	Provide product capability information; support concept development	Provide information about impact of change
Develop approval path	Lead definition of approval path, in collaboration with individual applicants where appropriate	Agree approval plan with approver	Review and accept approval plan	Develop safety argument modules as required to support approval path	Provide information about compliance with requirements	Provide information about impact of change
Develop solution	Lead development of solution at TAS level	Develop safety argument module and assurance contracts; generate evidence	*None*	Monitor argument and compliance with assurance contracts	Supply evidence to support relevant safety argument modules	Monitor impact of solution on organisation
Obtain approval	Co-ordinate applications for approval	Make application for approval	Review application and grant approval	*None*	Provide supplementary evidence as required	Provide supplementary evidence as required
Operational service	Monitor occurrences of precursor events or other incidents	Responsible for operation under terms of approval	Monitor operator's compliance with their SMS	Maintain argument based on monitoring of performance	Investigate occurrences of precursor events or other incidents	Monitor impact of operation on organisation

6 Conclusions

In response to the call to improve approval processes in the European aviation industry, the ASCOS Project has shown how modular safety arguments (as widely popularised in safety critical industries, assisted by the development of GSN) can be used to provide a flexible framework for developing safety arguments for changes to the Total Aviation System.

The ASCOS Method is a development of previous work by EUROCONTROL (EUROCONTROL 2010) and Single European Sky ATM Research (SESAR) (SESAR 2012), which introduced a high level safety argument for ATM safety cases. The developments here expand that work to ease its application across the TAS.

The ASCOS Method introduces a modular safety argument structure with modules aligned to domains and organisations within the TAS. Assurance contracts are used to capture and manage the dependencies between modules, addressing one of the critical issues in the development of safety arguments, where stakeholders make assumptions about parts of the TAS which are outside their control. Incorrect management of assumptions, especially those between domains, was a key concern which emerged from the research.

The modular safety argument framework allows approaches and techniques currently used to gain approval within European aviation to be retained where they remain applicable and provides guidance on how these approaches can be augmented where necessary to meet the challenges presented by the complex changes which are now being introduced.

This framework also recognises the importance of early co-ordination between all stakeholders in a change, including the applicant and the approver, to ensure that the safety argument and supporting evidence will be acceptable.

The ASCOS Method described here is the culmination of three years collaborative effort between the ASCOS participants. The method either addresses directly, or provides a framework for addressing, the principles and recommendations identified earlier within the project; further details are provided within the full description of the method (ASCOS 2015a). The report also makes a number of recommendations for development of supporting material and other activities which would support the implementation of the method, including:

- documentation of the implicit safety arguments currently used within aviation
- further definition of the domain structure of the TAS
- development of example safety arguments
- research into open sharing of safety risk information across the industry
- refinement of the TESG concept
- research into the trade-off of safety between domains

However, the most important next step is to apply the ASCOS Method to real life projects and use the experience from those projects to refine and improve the method.

Acknowledgments This technical publication has been realized partly with funding from the European Commission under the ASCOS (Aviation Safety and Certification of new Operations and Systems) Project (Grant Agreement No 314299). The support of the ASCOS consortium partners (see http://www.ascos-project.eu) and Dr Michael Kyriakopoulos, EC scientific officer for project ASCOS, is greatly appreciated.

Abbreviations and Acronyms

Acronym	*Description*
AAIB	Air Accidents Investigation Branch
AARS	Automated Aircraft Recovery System
AMC	Acceptable Means of Compliance
ANSP	Air Navigation Service Provider
ASCOS	Aviation Safety and Certification of New Operations and Systems
ATM	Air Traffic Management
CAA	Civil Aviation Authority
CNS	Communication, Navigation and Surveillance
CS	Certification Specification
EASA	European Aviation Safety Agency
EC	European Commission
FAA	Federal Aviation Administration
GSN	Goal Structuring Notation
JAM	Journal of Aviation Management
RPAS	Remotely Piloted Aircraft System
SESAR	Single European Sky ATM Research
SCSC	Safety Critical Systems Club
TAS	Total Aviation System
TESG	TAS Engineering and Safety Group
WP	Work Package

References

AAIB (2015) Report on the accident to Airbus A319-131, G-EUOE, London Heathrow Airport, 24th May 2013. https://www.gov.uk/aaib-reports/aircraft-accident-report-1-2015-airbus-a319-131-g-euoe-24-may-2013 Accessed 27th August 2015.

ASCOS (2013a) D1.2: Definition and evaluations of innovative certification approaches. https://www.ascos-project.eu/downloads/ascos_wp1_nlr_d1.2_version-1.4.pdf Accessed 17th September 2015.

ASCOS (2013b) D1.3: Outline Proposed Certification Approach. https://www.ascos-project.eu/downloads/ascos_wp1_ebe_d1.3_version-1.2.pdf Accessed 27th August 2015.

ASCOS (2014) D2.5: WP2 Final Report – Continuous Safety Monitoring. https://www.ascos-project.eu/downloads/ascos_wp2_ava_d2.5_version-1.3.pdf Accessed 11th September 2015
ASCOS (2015a) D1.5: Consolidated New Approval Method. https://www.ascos-project.eu/downloads/ascos_wp1_ebe_d1.5_version-1.1.pdf Accessed 20th October 2015.
ASCOS (2015b) D1.6: WP1 Final Report. https://www.ascos-project.eu/downloads/ascos_wp1_tr6_d1.6-version-1.3.pdf Accessed 20th October 2015.
ASCOS (2015c) D3.5a: Total Aviation System Safety Standards Improvements. https://www.ascos-project.eu/downloads/ascos_wp3_aps_d3.5a_version_1.4.pdf Accessed 17th September 2015.
ASCOS (2015d) D3.6: WP3 Final Report – Safety Risk Management. https://www.ascos-project.eu/downloads/ascos_wp3_aps_d3.6_version-1.2.pdf Accessed 27th August 2015.
ASCOS (2015e) D4.6: WP4 Final Report – Certification Case Studies. https://www.ascos-project.eu/downloads/ascos_wp4_nlr_d4.6_version-1.1.pdf Accessed 11th September 2015.
ASCOS (2015f) D5.5: WP5 Final Report - Validation. https://www.ascos-project.eu/downloads/ascos_wp5_dbl_d5.5_version-1.1.pdf Accessed 20th October 2015.
EASA (2010) Composite Aircraft Structure (AMC20-29 - Annex II to ED Decision 2010/003/R)
EASA (2015) Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes (CS25 Amendment 17 - Annex to ED Decision 2015/019/R), 2015
EUROCONTROL (2010) Safety Assessment Made Easier – Part 1 Safety Principles and an Introduction to Safety Assessment, Edition 1.0
FAA (2002) Commercial Airplane Certification Process (CPS) Study: an evaluation of selected aircraft certification, operations, and maintenance processes
Fenn J., Hawkins R., et al. (2007) Safety Case Composition Using Contracts – Refinements Based on Feedback from an Industrial Case Study. In: Redmill F. and Anderson T. (Eds) The Safety of Systems. Springer
Fowler D. (2015) Functional Safety by Design – Magic or Logic. In: Parsons M. and Anderson T. (Eds) Engineering Systems for Safety. SCSC
GSN Committee (2011) GSN Community Standard Version 1
Holloway (2015) Explicate '78: Uncovering the Implicit Assurance Case in DO-178C. In: Parsons M. and Anderson T. (Eds) Engineering Systems for Safety. SCSC
JAM (2014) Safety Management, Certification and the Extended Use of Composite Materials in Large Passenger Aircraft Structures. In the Journal of Aviation Management 2014.
SESAR (2012) Safety Reference Material, Edition 00.02.01, Project ID 16.06.01, 30th Jan 2012