AtkinsRéalis

Presenting Safety Arguments

Plan Design Enable

1

AtkinsRéalis

Learning Objectives

- To introduce the need for a structured argument in a Safety Case/Assessment
- To identify some practical problems encountered when trying to present safety arguments for complex systems
- To introduce graphical techniques (GSN & CAE) for developing and representing safety arguments
- Introduce ASPIRE AET Type Airworthiness Safety Assessment (TASA) Standardised Structure – AET Process 16
- To provide practical hints on reviewing safety cases/assessments
- To identify some potential flaws in safety cases/assessments.

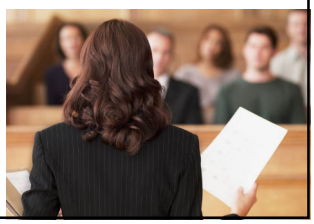
2

AtkinsRéalis

ASSC/Safety Assessment

- *Air System Safety Case (ASSC)= [1205(1)7] "Should consist of a claim (or a number of claims), a structured and explicit argument and a supporting body of evidence that together provide a compelling, comprehensible and valid case that an Air System is safe to operate and being operated safety within a clearly defined context (That is for a given application(s) in a given environment(s).*
- *[1205(1)8] It should begin at the concept stage with Safety arguments considered during capability design and selection and be managed through to and including disposal.*
- *Safety Assessment = "The Structured Argument that the system is safe for its intended use and that all applicable DLoD have been considered in the context of the overarching ASSC"* [MAA02]

- All definitions point to some evidence which is used to justify claims, the structured argument is used to provide the link between the two
- **Remember** - An argument without supporting evidence is unfounded, whilst evidence without argument is unexplained and therefore meaningless. [MASSC]



AtkinsRéalis

ASSC Report/ SCR

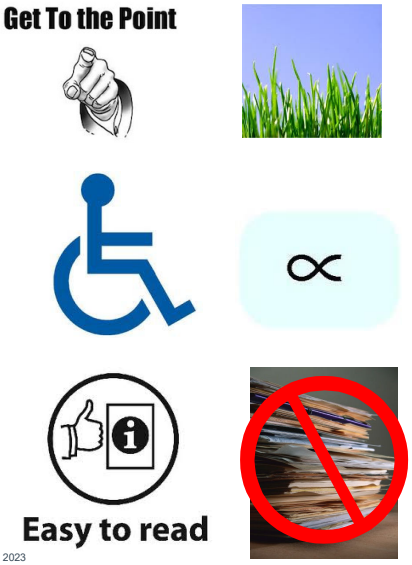
- ASSC Report = *[RA1205(1)16] "should be one document which captures the key components of the ASSC at a point in time; it should articulate the safety claim and the safety argument and summarize the supporting evidence in a clear and concise format".*
- *"The SCR is the means by which the project demonstrates that all of the safety issues relating to a project have been brought to a condition appropriate for the stage in the life cycle. It therefore provides the Safety justification to support the major Project milestones".*

[POSMS SMP12.1.2.2]

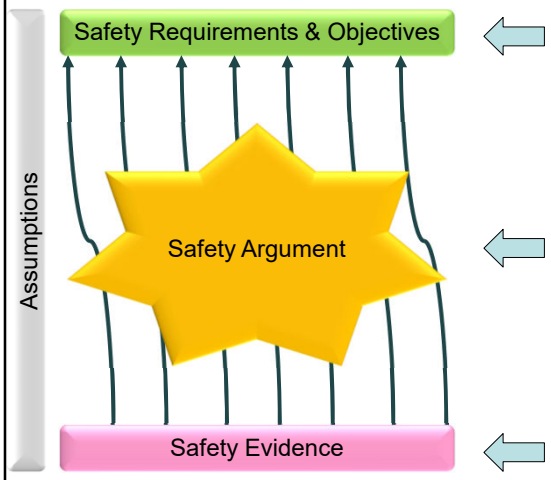
- The SCR provides a "snapshot" of the current Safety Case and shows those areas of significant risk
- Depth of evidence within a SCR **should be** commensurate with the system complexity and risk.

Reporting a Safety Case – SHAPED

- S – Succinct
- H – Home-grown
- A – Accessible
- P – Proportionate
- E – Easy to Read
- D – Document-Lite.



General Form of a Safety Case/Assessment



The Claims, Goals etc that we want to prove

The valid statements of fact which say why the claim has been met (based on the evidence)

The pieces of evidence that support the argument (test results, assurance reports etc..)

[Developed from MASSC]

AtkinsRéalis

Presenting Safety Cases/Assessments

- There are numerous ways to present Safety Cases/ Assessments including:
  - Traditional Textual Reports
  - Goal Structuring Notation (GSN)
  - Claims Arguments Evidence (CAE)
- Textual reports are fine but need to be logical and easy to read.

AtkinsRéalis

Safety Arguments – Text Example

The Defence in Depth principle (P65) has been addressed in this system through the provision of the following:

- **Multiple physical barriers between hazard source and the environment (see Section X)**
- **A protection system to prevent breach of these barriers and to mitigate the effects of a barrier being breached (see Section Y)**

...

- The text describes clearly how a safety requirement (P65) has been interpreted and achieved in the system
- It also clearly provides references to where the evidence supporting the lower level statements can be found
- Safety Arguments should clearly describe how a safety objective / requirement / claim has been achieved in the system
  - How it has been interpreted
  - Ultimately, what evidence supports the requirements.

Source Tim Kelly GSN – A Safety Argument Notation

AtkinsRéalis

Safety Arguments – Text Problems

> **For hazards associated with warnings, the assumptions of [7] Section 3.4 associated with the requirement to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 [4] that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.**

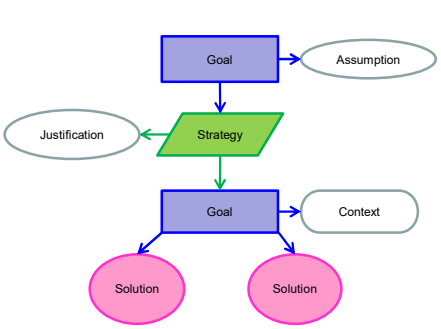
- Unclear & poorly structured - Not everyone can write clear English
- Can take many readings to decipher meaning
- Is there a clear shared understanding?

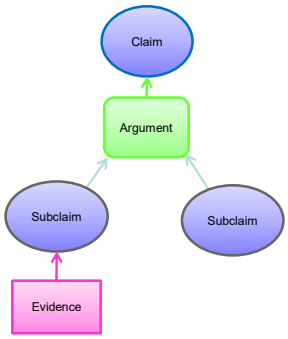
Source Tim Kelly GSN – A Safety Argument Notation

AtkinsRéalis

Presenting Clear Arguments

- It is possible in free text but:
  - Use simple language and short sentences
  - Use bullet points for key statements
  - Break down the argument one step at a time
  - Structure document sub-sections around separate concepts
- But it is easier with pictures e.g. GSN or CAE!



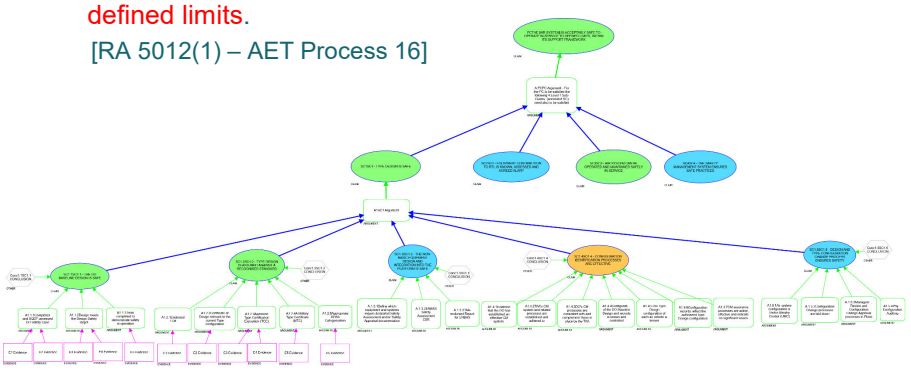


AtkinsRéalis

Type Airworthiness Safety Assessment (TASA)

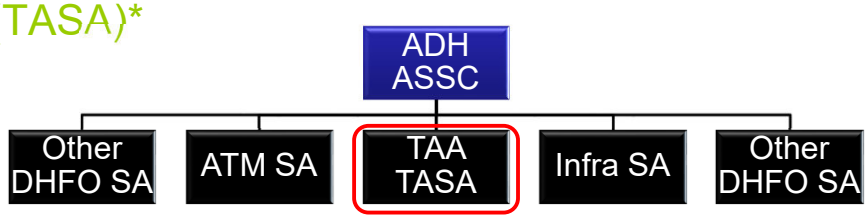
- The TASA should consist of a claim (or number of claims), a structured and explicit argument, and supporting body of evidence, that together provide a compelling, comprehensible and valid case in support of the ASSC that the Air System is safe to operate within defined limits.

[RA 5012(1) – AET Process 16]



AtkinsRéalis

Equipment Safety Assessment – Type Airworthiness Safety Assessment (TASA)*



Training
Equipment
Personnel
Information
Doctrine and Concept
Organisation
Infrastructure
Logistics

[AET Process 16 & RA 5012]

AtkinsRéalis

AET TASA CAE Argument – Process 16

TAA Declaration at 2* ESR

'Having presented evidence of strategies, plans and supporting arrangements, and the progress against them, I believe that the Air System covered by this Review is safe when maintained and operated in accordance with the Air System Document Set. All reported issues are being effectively managed and equipment hazards have been communicated to the Duty Holder.'

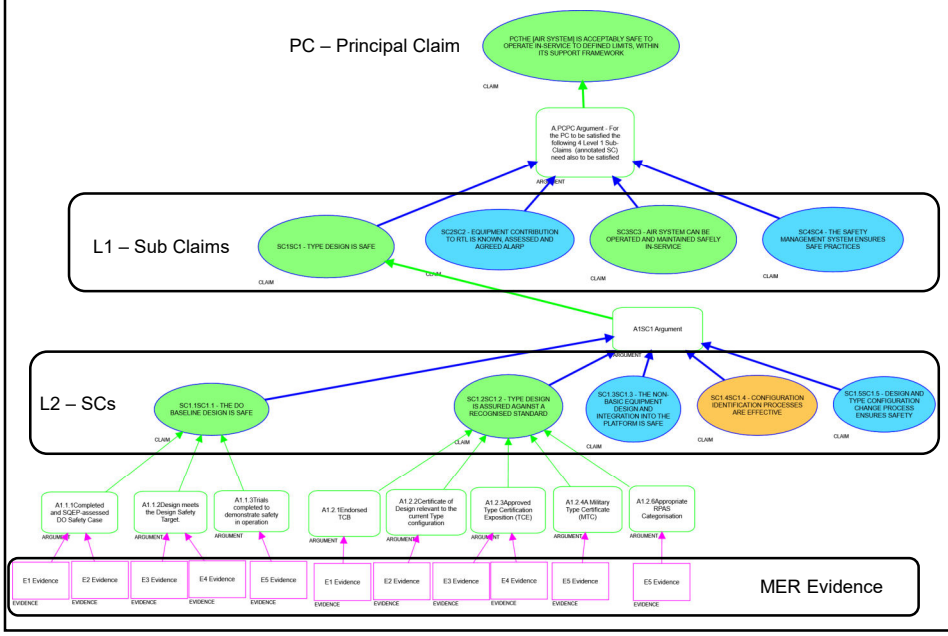
Principal Claim

XXXX Air System is Acceptably Safe to Operate in-Service to Defined Limits, within its Support Framework

TASA = Type Airworthiness Safety Assessment

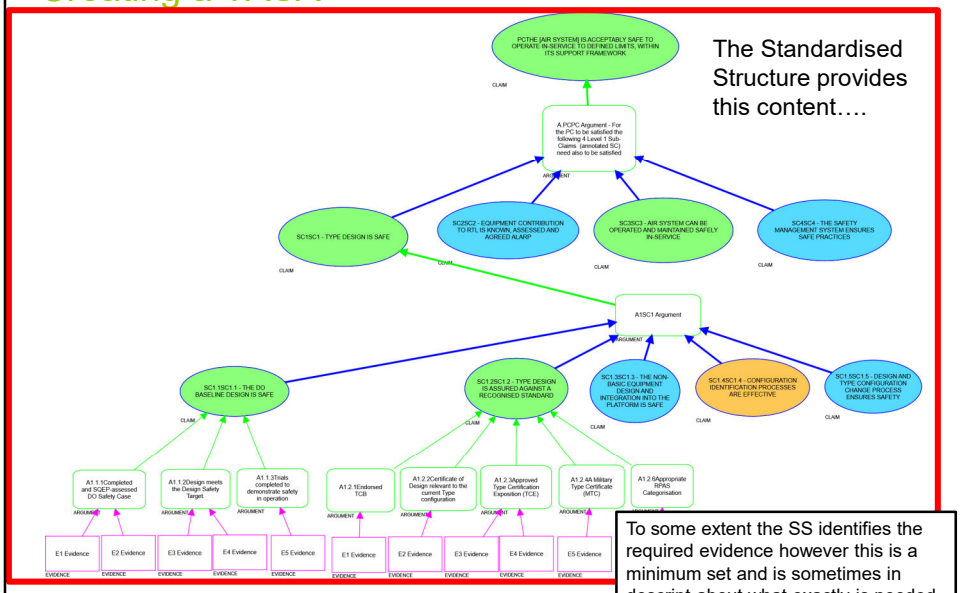
AtkinsRéalis

TASA Standardised Structure



AtkinsRéalis

Creating a TASA

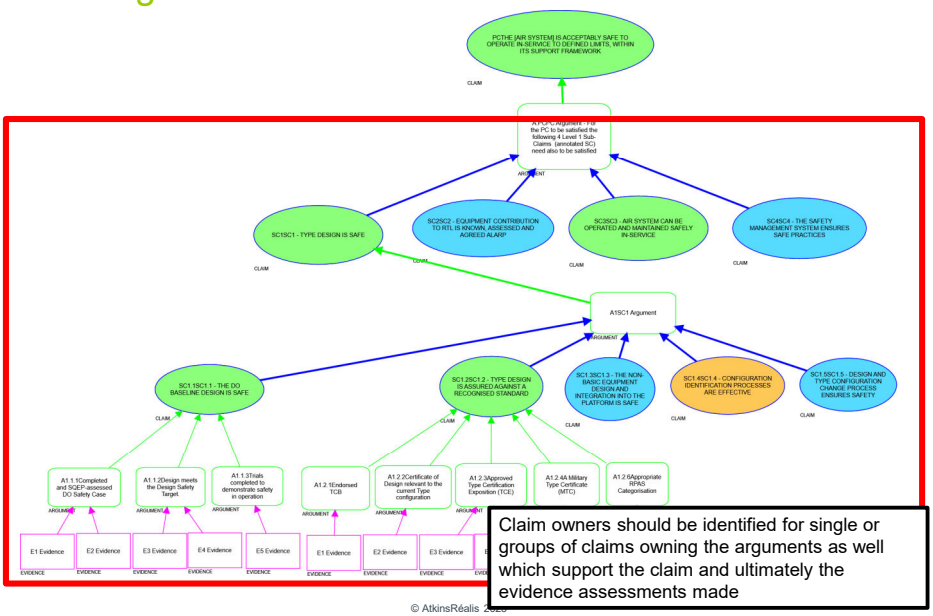


The Standardised Structure provides this content….

To some extent the SS identifies the required evidence however this is a minimum set and is sometimes in descript about what exactly is needed.

AtkinsRéalis

Creating a TASA

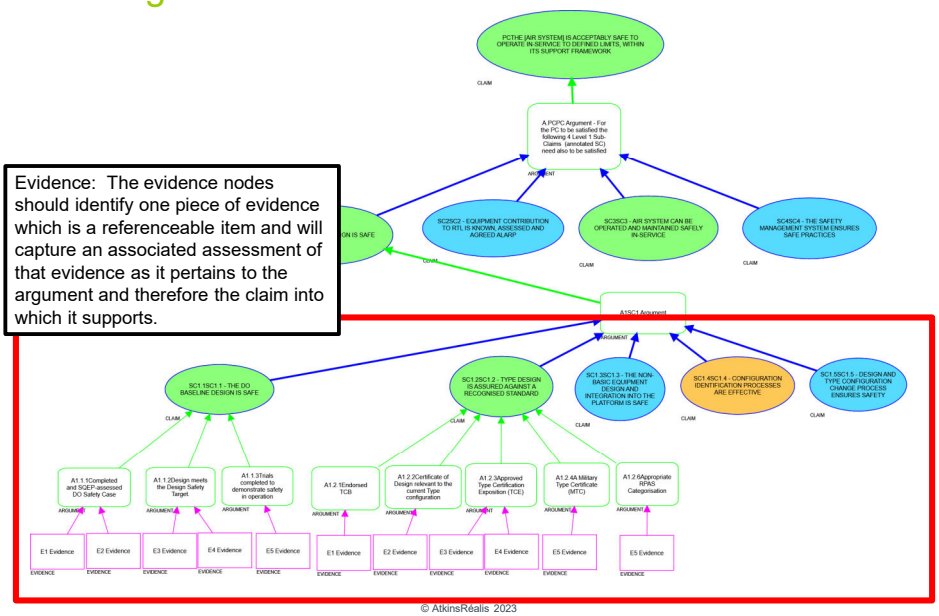


Claim owners should be identified for single or groups of claims owning the arguments as well which support the claim and ultimately the evidence assessments made

AtkinsRéalis

Creating a TASA

Evidence: The evidence nodes should identify one piece of evidence which is a referenceable item and will capture an associated assessment of that evidence as it pertains to the argument and therefore the claim into which it supports.



AtkinsRéalis

TASA Evidence - BGAR

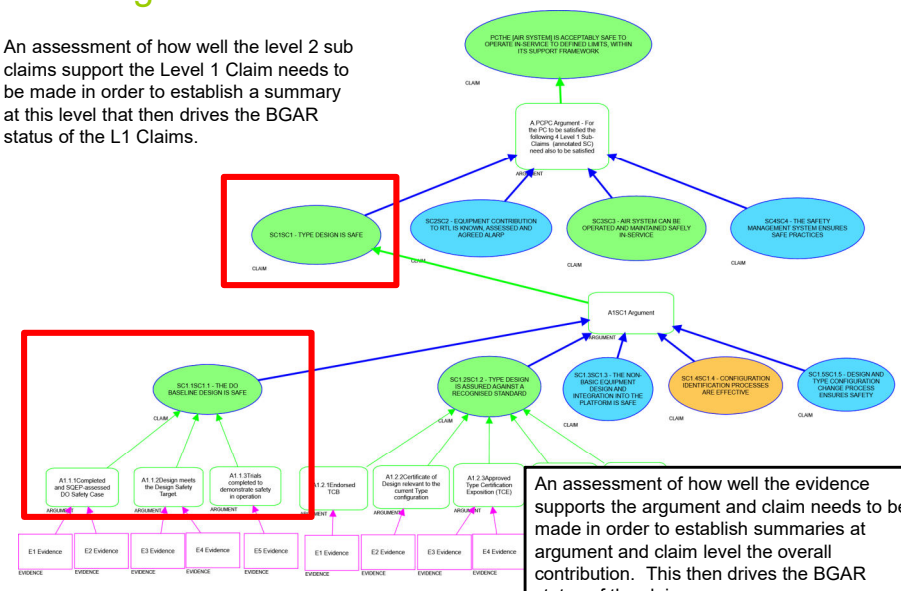
Evidence Criteria Definition Evidence within the TASA is provided with a confidence colouring as follows:	
BLUE	The evidence artefact has been reviewed and that the evidence supports the Claim.
GREEN	The evidence artefact supports the Claim, but there are associated recommendations to address minor shortfalls in the evidence.
AMBER	**In Service:** There is less confidence in the evidence artefact's ability to support the Claim. This could be as a result of the age of the defined evidence, its review status (i.e. under review or draft) or that review and/or Service experience has presented a minor challenge to its ability to support the Claim. **Development:** There is a possibility that evidence many not be established that fully supports the claim.
RED	**In Service:** There is poor confidence in the evidence artefact's ability to support the Claim. This could be because the evidence artefact is not in place or that review and/or Service experience present a significant challenge to its ability to support the Claim. **Development:** Evidence that supports the Claim is not expected to be available in the future or review has presented, or is expected to present, a significant challenge to its ability to support the Claim

[ASPIRE - AET Tool 16L]

AtkinsRéalis

Creating a TASA

An assessment of how well the level 2 sub claims support the Level 1 Claim needs to be made in order to establish a summary at this level that then drives the BGAR status of the L1 Claims.



An assessment of how well the evidence supports the argument and claim needs to be made in order to establish summaries at argument and claim level the overall contribution. This then drives the BGAR status of the claim.

AtkinsRéalis

TASA Claims - BGAR

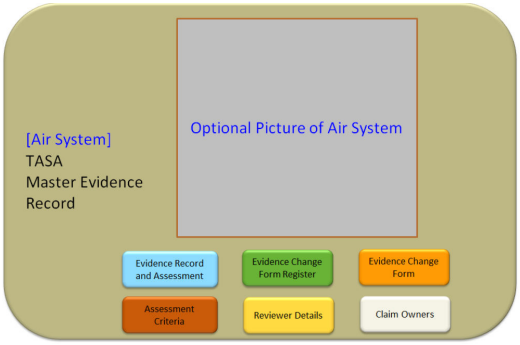
Claim Criteria Definition Claims within the TASA is provided with a confidence colouring as follows:	
BLUE	The Claim is substantiated. There is no shortfall and the argument is supported by contemporary, appropriate and sufficient evidence. No elevated Risk to Life.
GREEN	The Claim cannot be fully met. There is a Shortfall, that this is fully mitigated by effective controls. No elevated Risk to Life
AMBER	**In Service:** The Claim cannot be met. There is a shortfall that presents a potential Risk to Life, partially mitigated by additional controls. Duty Holder should be informed. **Development:** The Claim is unlikely to be met, with shortfalls which are likely to lead to an elevated Risk to Life later in the programme. Partial mitigations may be possible. Duty Holder consultation is likely necessary.
RED	**In Service:** The Claim cannot be met. There is a shortfall that presents and elevated risk to life requiring formal consultation with the Duty Holder. **Development:** The Claim will not be met at later stages in the programme. There will be a shortfall that will lead to an elevated Risk to Lide that will require consultation with the sponsor, and must be considered by the Duty Holder prior to operation of the Air System.

[ASPIRE - AET Tool 16L]

AtkinsRéalis

TASA Master Evidence Record (MER)

- MER assists DTs in:
  - Maintaining Evidence Configuration Status Record (CSR)
  - Assessing Evidence within the Master Evidence Report
  - Retaining an audit trail of changes to evidence and claim responsibility
- Contains Airworthiness info vital to TASA.



[ASPIRE - AET Tool 16L]

AtkinsRéalis

TASA Report or TASAR

- The TASAR is derived from the TASA that has been captured in ASCE or other environment and from the evidence assessments captured in the MER primarily but captured as a subset where required in the Evidence Assessment Narrative to the TASAR *[Enclosure 1 in the AET 16F TASAR Template]*.
- In addition, a graphical representation of the TASA CAE diagram is to be provided [Enclosure 2 to the TASAR].
- The AET Tool 16F provides a TASAR Template which complies with RA5012 and DS00-056 and will guide the author to capture and present the necessary elements of the TASA.
- TASARs are to be created where none exist and updated for 2 principle reasons:
  - When the evidence set changes and this significantly changes the current assessment of the TASA;
  - At least every 5 years.
- TASAR Addendums can be used to introduce minor changes to the evidence set where the TAA considers the changed insufficient to trigger a TASAR update.

AtkinsRéalis

TASA Status Report (TASA-SR)

- Pre PSEP a TAA chaired internal review is expected to be outputted into a TASA Status Report.
- ASPIRE requires a TASA-SR to be produced for each Project Safety & Environmental Panel (PSEP).
- TASA-SR should include the claim colour-coded assessments from the previous PSEP and provide a forecast colour-code for the next PSEP.
- The result of the PSEP is that the TASA-SR is reviewed and endorsed.
- TASA-SR used by TAA to provide current TASA assessment and justification info to inform the ADH's ASSC.
- A member of the DT will be responsible for all Sub-claims:
  - May require a LoAA or LoAN;
  - Assignment of responsibility illustrated in Safety Assessment..

[ASPIRE - AET Tool 16H]

AtkinsRéalis

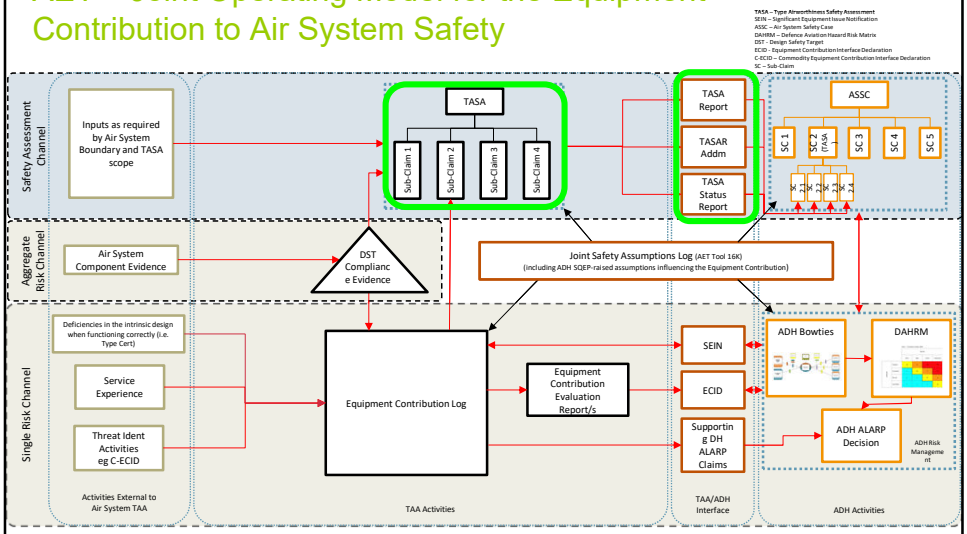
TASA-SR Example

Level 1 Claim Summary SC3		Previous	Current	Forecast	*[Provide an assessment of the status of the overall Sub-Claim. Any level 2 Sub-Claim that is not assessed as Blue/Green must be covered along with an assessment of the implications of the limited assessment.]*					
Claim Serial No.	**Level 1 Claim**	**Claim Assessment**			**Claim Serial No.**	**Level 2 Claim**	**Claim Assessment**			**Assessment Rationale**
3	Air System can be Operated and Maintained Safely In-Service	Previous	Current	Forecast	3.1	Operating Parameters are Known and Limits Defined	Previous	Current	Forecast	*[For all assessments give a short explanation of the rationale for the current assessment and provide details if the assessment has changed since the last report. Further instruction is given at the endnote.[ii]]*
					3.2	Actual Usage Reflects Authorised Limits	Previous	Current	Forecast	

[ASPIRE - AET Tool 16G]

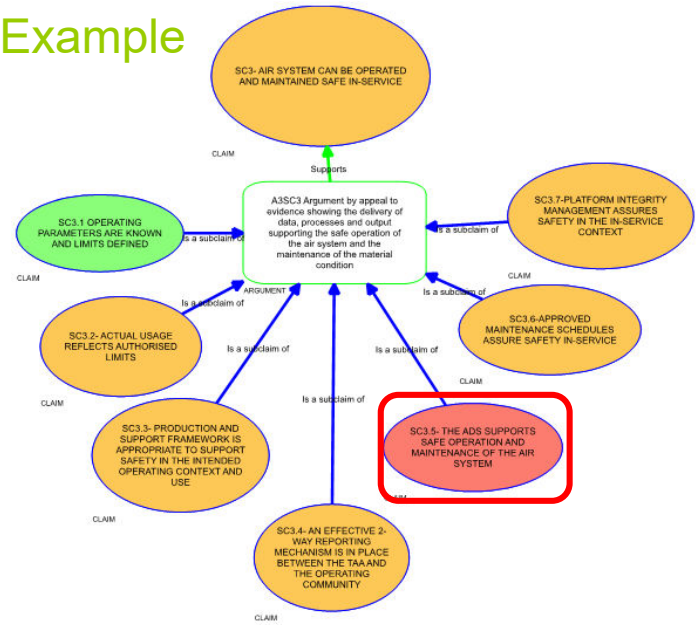
AtkinsRéalis

AET – Joint Operating Model for the Equipment Contribution to Air System Safety



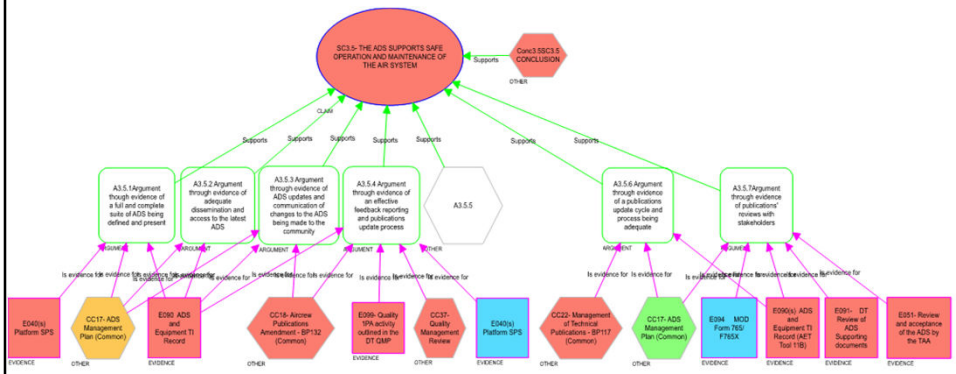
AtkinsRéalis

TASA Example SC3



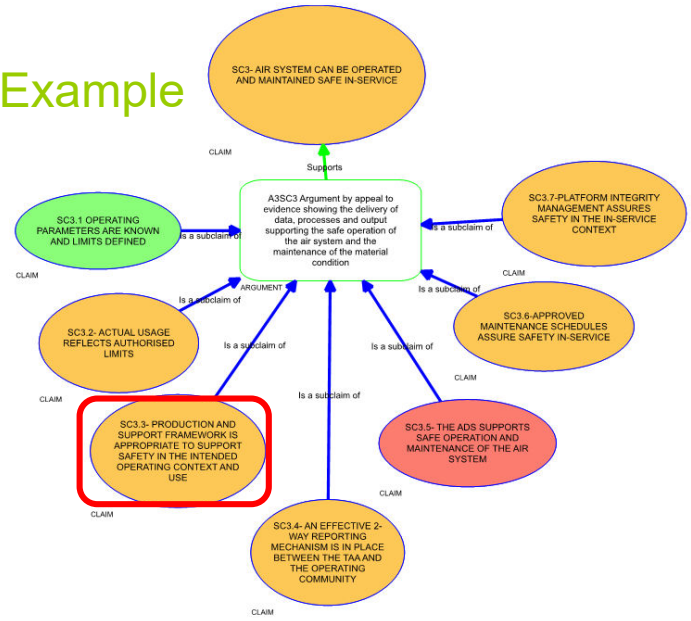
AtkinsRéalis

TASA Example SC3.5



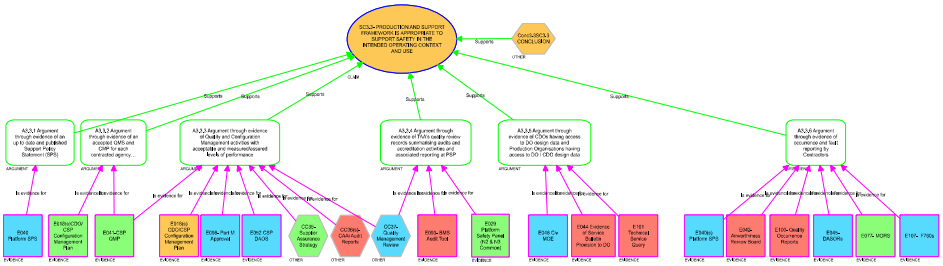
AtkinsRéalis

TASA ASCE Example



AtkinsRéalis

TASA ASCE Example SC 3.3



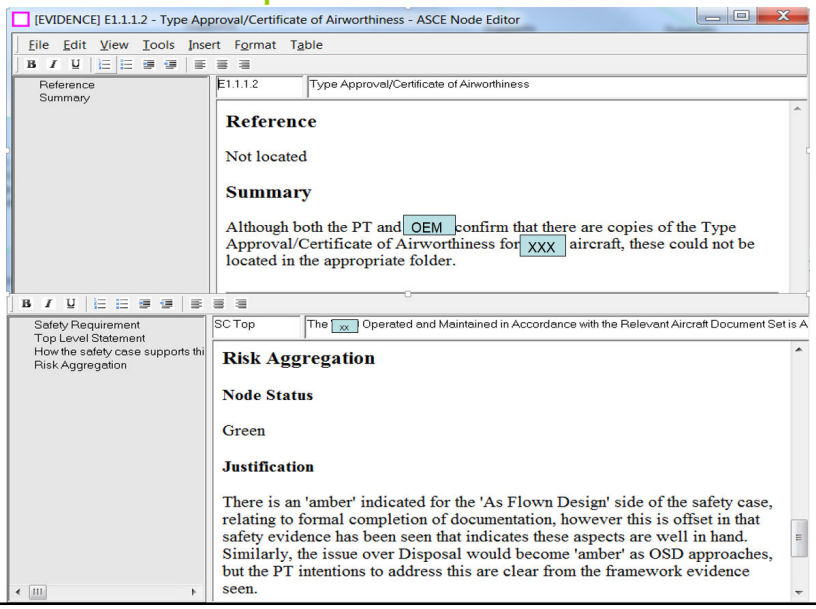
AtkinsRéalis

How is Evidence Used?

- Think about evidence used in legal (court) case
  - Direct - Supports a conclusion with no “intermediate steps”
    - e.g. a witness testifies that he saw the suspect at point X at time Y
  - Circumstantial - Requires an inference to be made to reach a conclusion
    - e.g. ballistics test proves the suspect’s gun fired the fatal shot

- TASA evidence is similar
  - e.g. Testing is direct – shows how the system behaves *in specific instances*
  - Conformance to design rules is indirect – allows inference that system is fit for purpose (if rules have been proven e.g. Claim that a system complies with Def Stan 00-970).

Actual Examples of Poor Practice



Things to Avoid

- ✘ The ‘apologetic’ safety case
  (Hiding system not safe)
- ✘ The ‘document-centric’ view
  (Document becomes the goal)
- ✘ The approximation of truth
  (Smooths over ‘rough’ bits)
- ✘ The prescriptive safety case
  (Shoehorned into template)
- ✘ The safety case as ‘shelf-ware’
  (SC not actually used)
- ✘ Imbalance of skills
  (DT/MAA not qualified to challenge)
- ✘ The illusion of pictures
  (Reviewer dazzled by graphics).

[Source: Dr Tim Kelly in H-C Nimrod Report]

Summary

- The objective of the SC/A is to 'pull together' many forms of information and present a coherent argument of safety
- Problems of scale and complexity:
  - 'Chain of argument' can often get lost
- Graphical methods, e.g. GSN/CAE, can be a useful means of presenting safety arguments:
  - Safety case "patterns" can help by allowing re-use of strong / successful arguments – Basis of ASPIRE methodology
- Production of SC/A must not be left until the end of a project:
  - SC should be evolved through the phases of project development
  - Developing argument early in project can help define safety activities to ensure necessary evidence is produced and avoid wasting time and money on activities that do not contribute to the SC.

Questions?