

Presentation of Safety Arguments a Regulator's Perspective

Stephen Barker
Safety Assessment Engineer
Air Traffic Standards Division (ex-department)
Civil Aviation Authority, Safety Regulation Group

Contents

Background

Where I'm looking from

Structured Arguments

CAE, GSN, Use, Tools ...

Our use of ASCE

References

Disclaimers

Not partisan regarding use of either CAE, GSN, or ASCE

Personal views, not 'official CAA SRG' position

My experience with ASCE, CAE & GSN

Originally sceptical of necessity

Only first level of familiarity with GSN

Used ASCE & CAE to co-operatively create intellectually demanding arguments

Reviewed a number of submissions using CAE

Standalone SW01 and overall safety arguments

GSN is proselytising heavily

Civil Aviation Authority (CAA)

- Economic Regulation Group (ERG)
- Department of Airspace Policy (DAP)
- Consumer Protection Group (CPG)
- **Safety Regulation Group (SRG)**

- Airworthiness Division
- Flight Operations Division
- Licensing Standards Division (LSD)
- **Air Traffic Standards Division**

— Strategy & Standards

— **CNS/ATM Standards**

— International Coordination and Standards

— **Operations**

— **En-Route and ATS College Regulation**

— **3 Regional Offices (Stirling / Manchester / Gatwick)**

— ANSP Certification



SW01
used

Air Traffic Standards Division

Safety regulation of civil “Air Traffic Control” in UK

Centres (Swanwick, West Drayton, Prestwick)

Infrastructure

Airports (from Heathrow to Little Snoring)

Equipment, People, Procedures

65 people

Management, Administrative, Controller, Engineer

ATS Equipment

Bespoke (£££££) e.g. radar, workstations

COTS (£) e.g. radios, recorders, infrastructure components

No mandatory development / assurance standards

Goal-based regulation

Permissioning regime – SMS – audit



CAP 670 Part B Section 3 SW01

Regulatory Objectives for Software Safety Assurance in ATS Equipment

First appeared as guidance in CAP 581 1997 (became CAP 670 in 2001)

Mandatory since 23 Dec 2002

Five mandatory objectives – RV, RS, RT, NI, CC

Guidance

SW01 requirements

Arguments (a set of reasons given in support of something)

Evidence (direct and backing)

Tolerably safe

“To ensure that **arguments** and **evidence** are available which show that the Software Safety requirements correctly state what is necessary and sufficient to achieve **tolerable safety**, in the **system context**”

Safety arguments

DS 00-56

“A Safety Case is a **structured argument**, supported by a body of **evidence**, that provides a compelling, comprehensible and valid case that **a system is safe for a given application in a given environment.**”

What is an argument?

A set of reasons given in support of something

What is its purpose?

To persuade, to convince

To critically evaluate the validity of one's own beliefs

And

Record safety rationale for later use

A 'living document'

Structured arguments – general comments

Neutral policy on use of structured arguments, but ... we like them

- Clarity, focus, relationship between various subjects

- Difficult to equal using plain prose alone

CAE can be used as a contents list, an overview of the argument

Can a diagrammatic presentation replace the safety case, rather than augment it?

GSN node text is extremely brief – can you persuade so succinctly?

- A work breakdown structure is not an argument

Lessons from code-generating CASE tools?

Complexity

What is the argument?

The diagram and the text?

Does the diagram only support the text?

The diagram's text augmented by the diagram semantics?

Teams have mixture of skills and experience.

E.g. in ATS there are many technical specialists (e.g. radar, landing aids, controllers!) and managers

Dilemma over richness of syntax and semantics

Want expressive notation, with clearly defined meaning

Syntax and semantics need to be simple and intuitive, not complex and esoteric

e.g. inheriting scope or context

Authors prefer sub-arguments to be completely standalone / self-consistent / portable => finished

Creation

Argument often only properly written well into the project

Often when activities and budgets fixed

Need better safety planning – draft safety arguments earlier in the process

Want to baseline at certain levels of detail, but often find that further level development involves revisiting higher level arguments

Is this confined to CAE?

When returning to an earlier argument, it is difficult to ‘tune in’ and concur with what was written, and not rewrite

Consequences for teams of authors

CAE – confusion over the difference between C & A

Reviewing structured arguments

Do not find reviewing them easy

Have to 'tune in' to argument

Style - difficult to differentiate substantive comments from "I wouldn't put it like that"

Difficult to concur at one level without understanding 'what lies beneath'
'the devil is in the detail' or just natural regulatory cynicism?

Difficult to keep place when a review is interrupted.

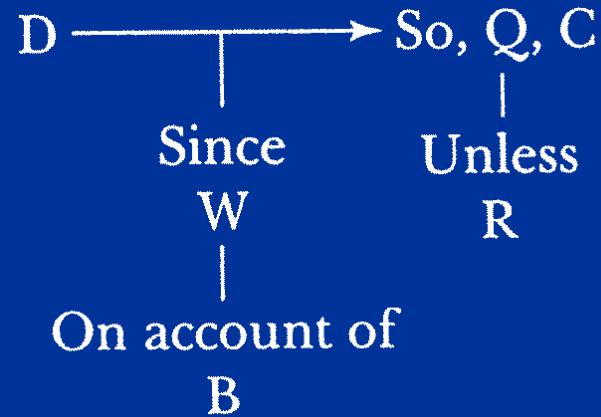
Confusion with structured software

Unsupported assertions

expert opinion in a formal document?

Are these just goal-based regulation, rather than structured argument issues?

Argument 'scale'



Do CAE and GSN work better at different scales?

Of what I've seen:

Much of GSN is large scale, low complexity e.g. overall project adequacy
Most CAE is detailed software safety arguments

'Toulmin' level arguments are within CAE argument nodes

But even then not that detailed

Surely not right that such detail is translated into diagrams?

Do we understand the relationships between these argument scales?

Should we seek to represent these relationships explicitly?

GSN (views of an ‘enthusiastic amateur’)

Seems too terse

Short strategy box text

If GSN shorter than CAE, where has the information gone?

Too easy to forget to make arguments for appropriateness / adequacy

‘Strategy’ is an assertion: “argument by satisfaction of all safety requirements” - no rationale / argument – intuitively obvious?

Logical inclusion of direct and backing arguments / evidence

Is GSN used by default because of familiarity?

Formalises separation of different aspects (clarity)

E.g. justification of argument validity from the argument itself

Are many pages of diagrams easy to understand? Context?

CAE

Arguments can get very long if they include justifying each step (i.e. model and strategy) of argument, as well as the argument itself

‘Other’ node is sometimes used to separate out one aspect e.g. context, justification

Received little attention in papers

Are the merits of GSN so clear-cut? If so, has anyone documented the reasons?

Is CAE just too simple to study?

Essence is presentation of an argument to support a claim

cw GSN's essence appears to be presentation of a strategy to achieve a goal

Tendency to have large bottom level arguments

Lots of evidence supporting

Tools

Relationship of tool content and project baselines

Arguments are written assuming 'success'

Freezing a snapshot for formal issue

User views – are they complete?

especially when reviewing

Cannot mandate

Suggestions for ASCE

On-line browser for locked-down desktops

Repeated nodes (evidence)

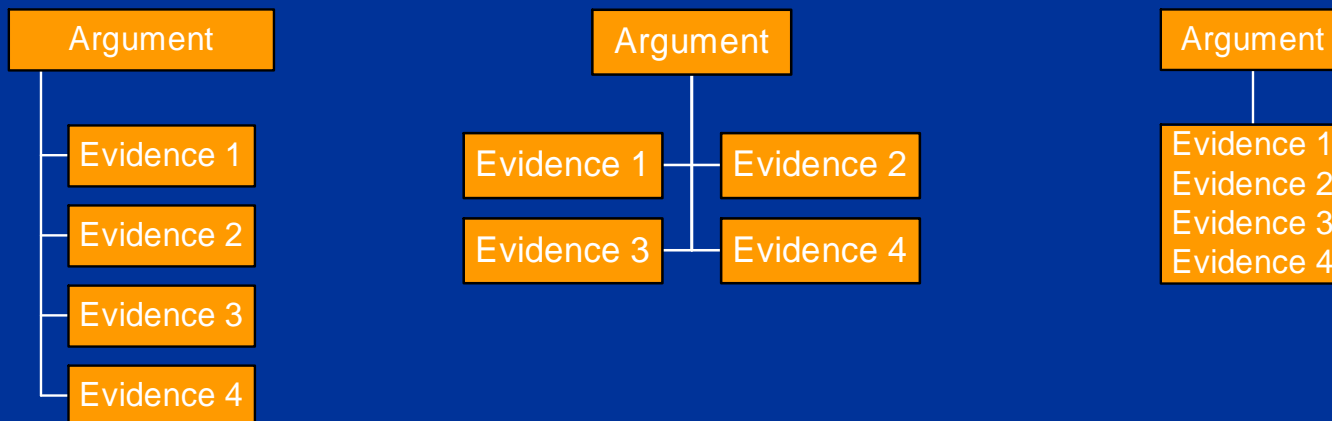
Printable Bird's-Eye view

Would like review mark-up layer in tools

Auto-user view - Immediate parent(s) and children in each arg node

Listing lots of evidence

Perhaps options like organisation charts



What (on earth) are we are doing?

Guidance on complying with SW01 for COTS, Changes to Legacy Systems
Not yet public domain

“The difficult part in an argument is not to defend one's opinion, but rather to know it.” - Andre Maurois [A Little Book of Aphorisms]

Much of our arguments are about models => GSN model node
i.e. validity of the warrant = backing (Toulmin)

Observed *modus operandi*

1. Model (taxonomy, entity relationship diagram)
2. Reason about related entities in the Model to get a Rationale
3. Refine it to get an argument, using ...
4. The evidence are items that appear in the ERD

Regulatory references

Air Traffic Standards Safety Requirements CAP 670

Includes Part B Section 3 SW01 – Regulatory Objectives for Software Safety Assurance in ATS Equipment

<http://www.caa.co.uk/docs/33/CAP670.PDF>

The Practicalities of Goal-Based Safety Regulation

J Penny, A Eaton, PG Bishop, RE Bloomfield

http://www.adelard.com/papers/scsc2001_sw01.pdf

Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases: For Aerodrome Operators and Air Traffic Service Providers

Includes “Appendix E Diagrammatic Representation of Safety Arguments”

<http://www.caa.co.uk/docs/33/CAP760.PDF>

A final thought

“How easy it was to mistake clear reasoning for correct reasoning!”

from ‘Dune Messiah’ by Frank Herbert - Hayt (Duncan Idaho) in
‘Mentat’ hyper-logical thinking mode