Research Report IFIP WG 10.4 Buzios Brazil June 2015

Besed on Shonan talk January 2015

On The Interpretation and Evaluation of Assurance Case Arguments

John Rushby

Computer Science Laboratory
SRI International
Menlo Park, California, USA

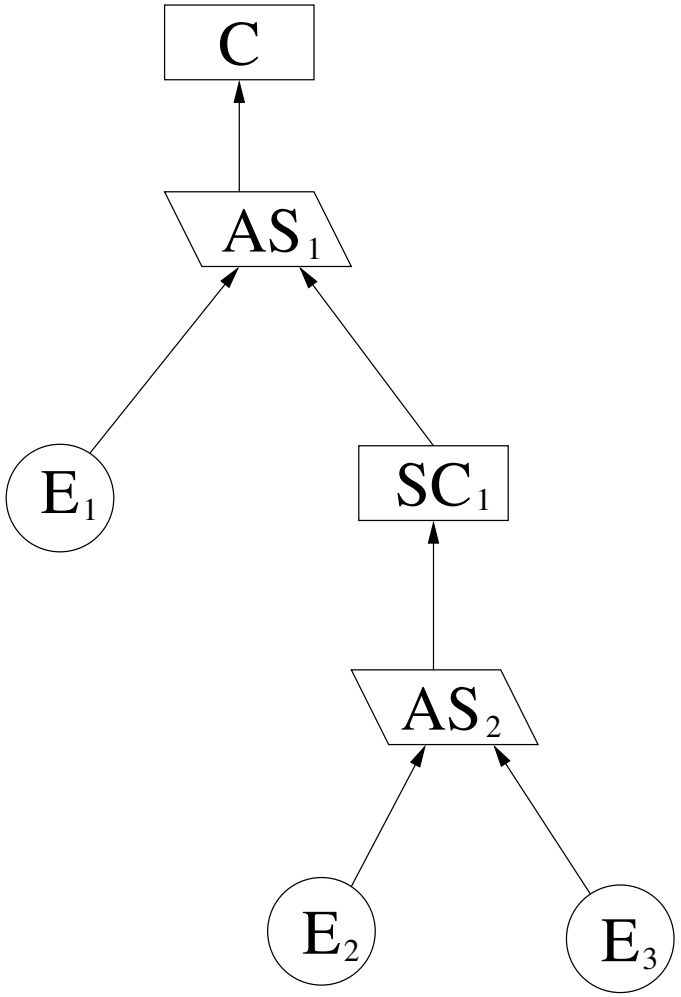
Assurance Case Arguments

- The idea is that we "make the case" to justify deployment of some system by
  - Stating the claim that it must satisfy
    - ⋆ Often safety-related
  - Developing evidence about its assumptions, design, performance etc.
  - Constructing as structured argument that justifies the claim, based on the evidence

- How should we interpret these arguments?
  - i.e., what are their semantics?

- And how do we tell if an argument is (sufficently) sound?

Structured Argument



C: Claim

AS: Argument Step

SC: Subclaim

E: Evidence

A hierarchical arrangement of argument steps, each of which justifies a claim or subclaim on the basis of further subclaims or evidence

Inductive and Deductive Arguments

- The world is an uncertain place (random faults and events)
- Our knowledge of the world is incomplete, may be flawed
  - Our reasoning may be flawed also
- So an assurance case cannot expect to prove its claim
- Hence, the overall argument is inductive
  - Evidence & subclaims strongly suggest truth of top claim
- Rather than deductive
  - Evidence & subclaims imply or entail the top claim
- But if the overall argument is inductive
  - Does that mean all its steps may be inductive too?
- That is, we necessarily have doubts
  - But where may they be located?
  - And how are they controlled?

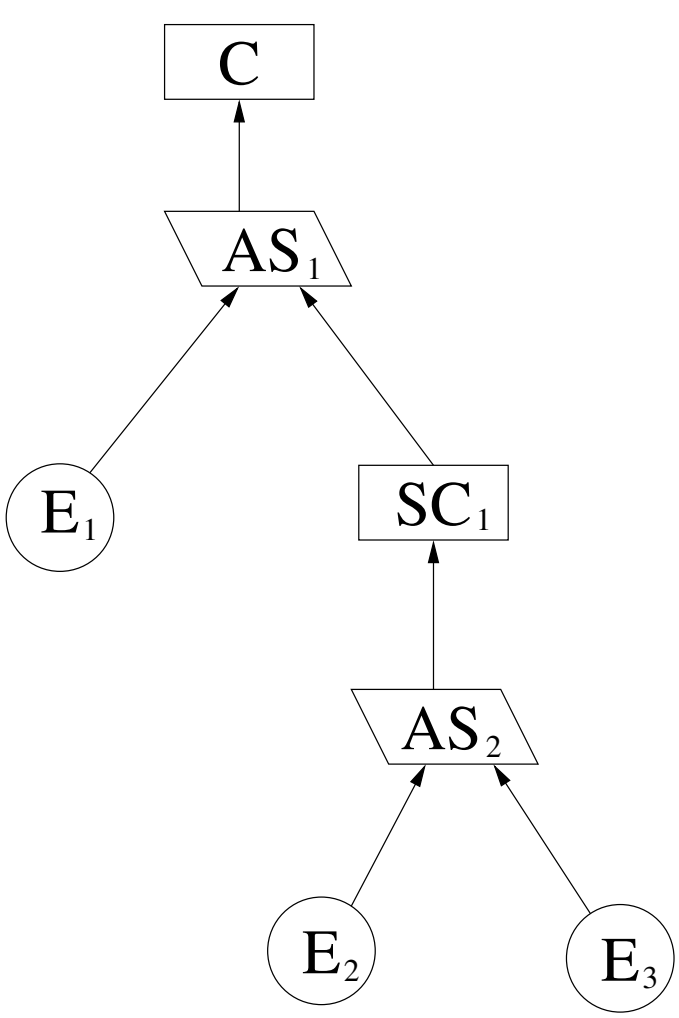
Traditionally. . .

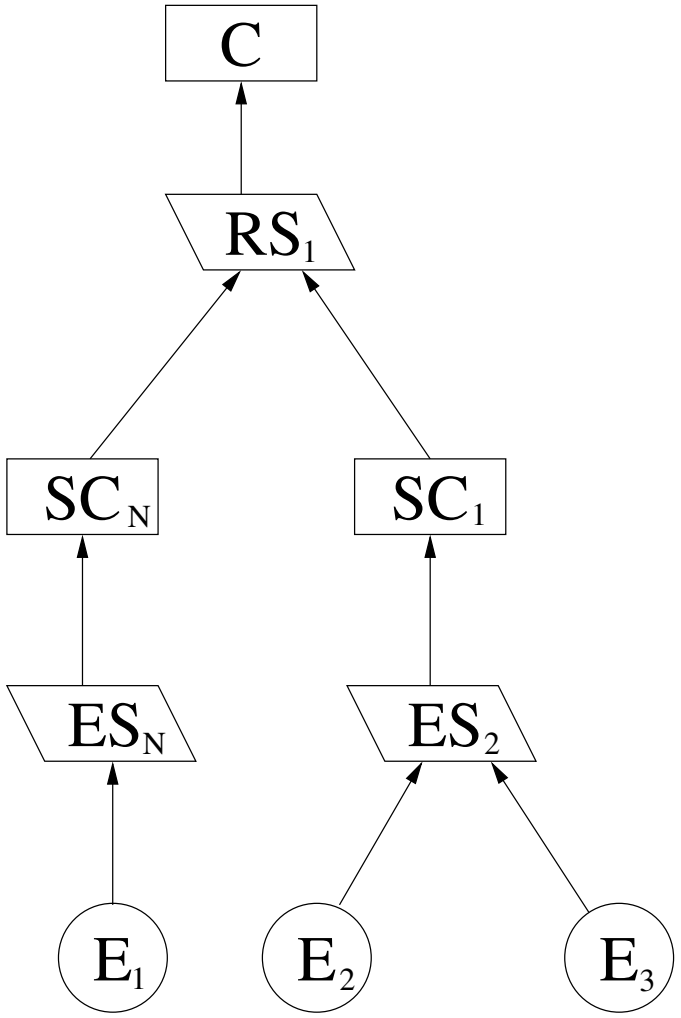
- Traditionally, every argument step can be inductive
- Considered unrealistic to be completely certain
  - cf. ceteris paribus hedges in science
- Then there's a tricky notion of confidence items
  - Evidence or subclaims that do not directly contribute to the argument
  - i.e., their falsity would not invalidate the argument
  - But their truth increase our confidence in it
- Eh?

Argument Steps and Layered Arguments

- We decompose top-level claim into conjunction of subclaims
- And iterate
- Until we get down to subclaims supported by evidence
- Provide a narrative justification for each step
- Can normalize so there are just two kinds of argument steps
  - Reasoning steps: subclaim supported by further subclaims
  - Evidential steps: subclaim supported by evidence
    - ⋆ Can allow claims as assumptions on evidential steps
- Call this a simple form argument

Normalizing an Argument to Simple Form





RS: reasoning step; **ES**: evidential step

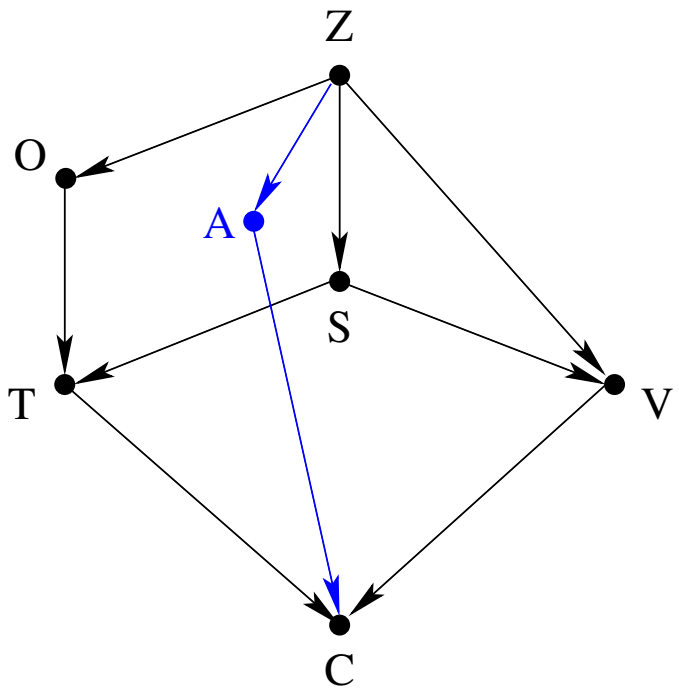
Why Normalize In This Way?

- Because the two kinds of argument step should be interpreted differently
- Evidential steps
  - These are about epistemology: knowledge of the world
  - Bridge from the real world to the world of our concepts
  - Have to be considered inductive
  - Multiple items of evidence are "weighed" not conjoined
  - Confidence items can be part of the weighing
- Reasoning Steps
  - These are about logic/reasoning
  - Conjunction of subclaims leads us to conclude the claim
    - ⋆ Deductively: subclaims imply claim
    - ⋆ inductively: subclaims suggest claim
  - Very hard to see what confidence claims do

Weighing Evidential Steps

- We measure and observe what we can
- To infer a subclaim that is not directly observable
- Different observations provide different views
  - Some more significant than others
  - And not all independent
- "Confidence" can be observ'ns that vouch for others
  - Or provide independent backup
- Need to "weigh" all these in some way
- Probabilities provide a convenient metric
  - And Bayesian methods and BBNs provide tools
  - There's also Bayesian Confirmation Theory
- I do not think the exact numbers and methods are important
  - Use BBNs for what-if investigations
  - To help develop insight and sharpen judgement

Weighing Evidential Steps With BBNs



Z: System Specification

O: Test Oracle

S: System's true quality

T: Test results

V: Verification outcome

A: Specification "quality"

C: Conclusion

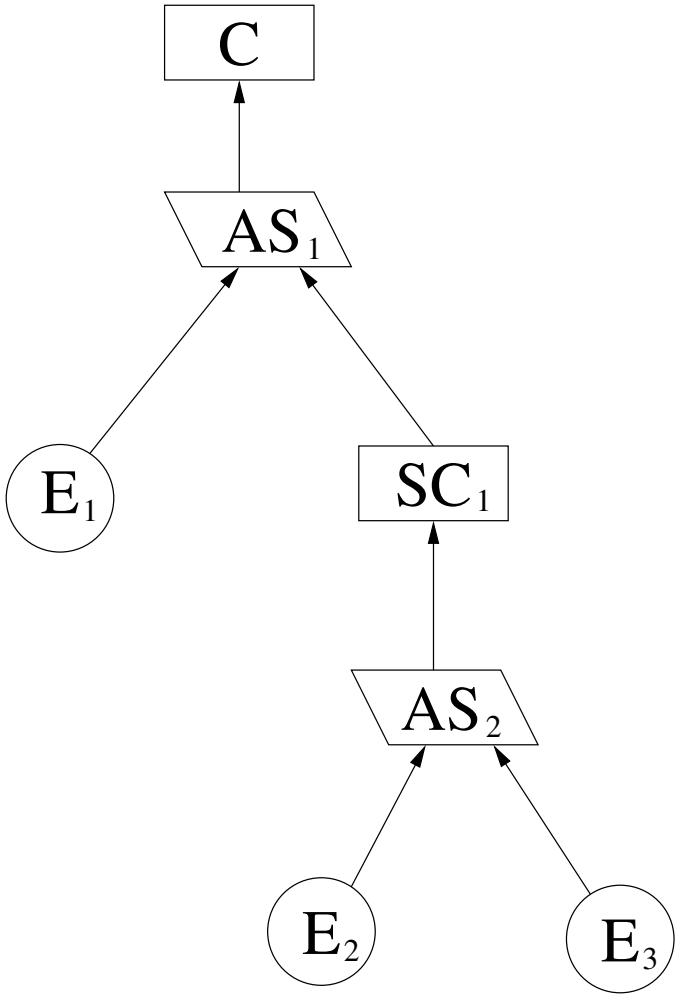
Example joint probability table: successful test outcome

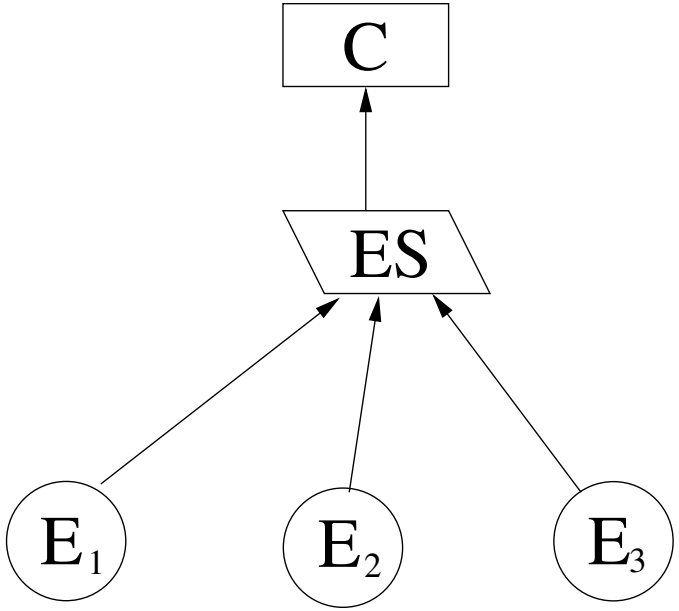
Correct System		Incorrect System	
Correct Oracle	Bad Oracle	Correct Oracle	Bad Oracle
100%	50%	5%	30%

Evaluating Reasoning Steps

- We could replace each subclaim by its supporting evidence
- Thereby flattening the argument
- And then apply BBNs to the whole lot

Collapsing an Argument





Evaluating Reasoning Steps (ctd.)

- There's a reason we don't do this
  - An assurance case is not just a pile of evidence
    - ⋆ That's DO-178C, for example
  - It is an argument
  - With a structure based on our reasoning about the system

- So the reasoning steps should be interpreted in logic
  - As conjunctions that imply or suggest their parent claim

Validating Reasoning Steps with Defeaters

- Validate reasoning steps by trying to think of defeaters
  - Circumstances where subclaims hold but claim does not
  - It's like hazard analysis, but applied to arguments
- Can do this ourselves, or in dialog with reviewers
- Do not challenge the individual subclaims
  - Those are validated (recursively) at lower levels
  - Treat them here as settled facts
- Look for gaps in the conjunction
- And fill them in with additional or modified subclaims
- This will tend to make inductive steps deductive
  - By finding the gaps or "assurance deficits"
  - Subclaims are of our own choosing, so choose well
- My opinion is that all reasoning steps should be deductive
  - Inductive is too low a bar, too fungible, indefinite

Evaluating the Soundness of an Argument

- Arguments should be in simple form
- Reasoning steps should be deductive
  - Evaluate by actively seeking defeaters
  - No role for confidence claims in reasoning steps
    - ⋆ "voluminous, rambling, ad infinitum arguments"
- Evidential steps are evaluated by weighing the evidence
  - Can also be challenged by seeking defeaters
  - Evidence may include confidence items
  - Weighing can be done informally
  - Or formalized and mechanized with BBNs
  - Must cross some threshold so that reasoning steps can regard evidential claims as settled facts
- Overall case is then sound

Graduated Assurance

- Many cert'n regimes recognize different levels of criticality
- Less assurance required for lower levels
- Assume the high level case is sound
  - We deliberately weaken it for lower levels
  - So those cases cannot be sound
  - How to do this responsibly?
- Remove some subclaims?
  - Equivalently, retain but require no evidence
  - Wrecks the model: reasoning steps no longer deductive
- Weaken evidence?
  - Lower the bar for settled facts
  - Seems acceptable, but must do it evenly
- Build a different case?
  - E.g., DO-178C without low level specifications
  - Also seems acceptable

Evaluating the Strength of an Argument

- Although I don't advocate flattening then BBNs
  - As a way to evaluate soundness of an argument
- It could be a way to quantify strength of a sound argument
- More simply
  - Just sum (Adams' Uncertainty Accumulation)
  - Or multiply (independence assumption)

  The probabilities calculated (by BBNs) for evidential steps
- Beware of gaming:
  - Combining subclaims to maximize strength measure
- Could do this on an ordinal scale (low, medium, high, etc.)
- Note that it's a weakest link calculation
- Graduated assurance retains soundness, reduces strength

Conclusion

- Interpretation is a combination of probability and logic
- (Possibly informal) probabilities for evidential steps
- Logic for reasoning steps
- Case is sound **if** evidential steps cross some threshold **and** reasoning steps are deductively valid
- Validate by seeking defeaters
- Graduated Assurance may weaken evidential support
- But must not eliminate subclaims or their evidential support
- Overall strength of a sound case is determined by weakest evidential step
- Can formalize this in probability logic, but I think the real appeal has to be to intuition and consensus. . .
- What do you think?

Links

- Lengthy report: http://www.csl.sri.com/users/rushby/papers/sri-csl-15-1-assurance-cases.pdf

- VeriSure Workshop (part of CAV) on "What is an Assuance Case," 18 July 2015, San Francisco: http://fm.csl.sri.com/verisure