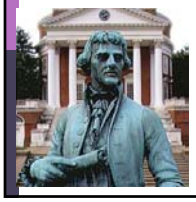
Assurance Cases:
New Directions & New Opportunities*

John C. Knight
Department of Computer Science
University of Virginia



February, 2008

***Funded in part by:**
the National Science Foundation & NASA

Outline

- A summary of several research topics from our group at UVA
- Topics covered:
  - Assurance argument fallacies
  - Accident investigation
  - Assurance based development
  - Assurance based communication
  - New directions in certification
- More details available from papers

Things I Like
Safety-Critical Systems

Outline

- **Assurance argument fallacies**
- Accident investigation
- Assurance based development
- Assurance based communication
- New directions in certification

The Safety Case

"…***comprehensive*** and ***defensible*** **argument** that a system is ***acceptably safe*** to operate in a ***particular context***." [T. Kelly]

- The safety case ***communicates***:
  - High-level safety objectives
  - Evidence that objectives have been met
  - Argument linking evidence to objectives
  - Assumptions, justifications, and other context
- Does it always ***communicate***:
  - Accurately?
  - Completely?

Assurance Case Has To Be Right

- Can we construct arguments that are free of fallacies?
- Can we check arguments?
- What is the effect of a fallacy?
- What should certifiers do with assurance cases?
- Let's look at some published assurance cases (actually safety cases)

Safety Case Survey

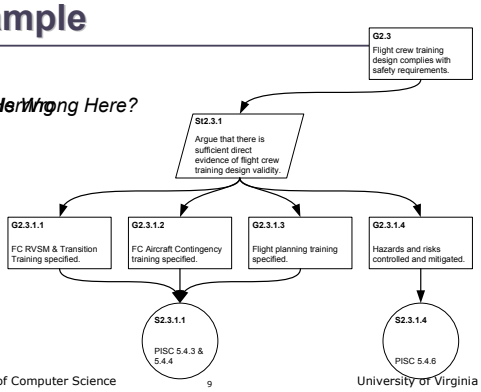
- Examined three industry safety cases:
  - Eurocontrol RVSM Pre-Implementation SC
  - Eurocontrol Whole Airspace ATM SC
  - Opalinus Clay Waste Repository SC
- Two reviewers noted frequency and nature of fallacies observed in each safety case.

Eurocontrol RVSM

Reduced Vertical Separation Minimum

Fallacy	A	B	Total
Using the Wrong Reasons	5	15	16
Drawing the Wrong Conclusion	3		3
Red Herring	1		1
Fallacious Use of Language	2	2	4
Hasty Inductive Generalization	4		4
Omission of Key Evidence		1	1
Total	15	18	29

Fallacious Argument Example



Arguing From Ignorance?

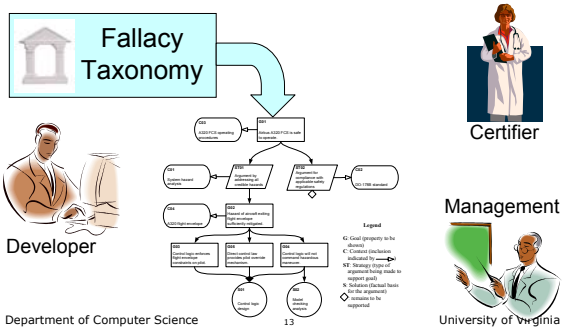
> **8.2.8.4 Absence of outstanding issues with the potential to compromise safety**
>
> The current safety analysis, despite a wide range of assessment cases that were derived in a careful and methodical way, has not identified any outstanding issues with the potential to compromise safety.
>
> Opalinus Clay Safety Case

So go ask the philosophers…

Assurance Case Fallacy Taxonomy

- Circular Reasoning
  - Circular Argument
  - Circular Definition
- Diversionary Arguments
  - Irrelevant Premise
  - Verbose Argument
- Fallacious Appeals
  - Appeal to Common Practice
  - Appeal to Improper/Anonymous Authority
  - Appeal to Money
  - Appeal to Novelty
  - Association Fallacy
  - Genetic Fallacy
- Mathematical Fallacies
  - Faith in Probability
  - Gambler's Fallacy
  - Insufficient Sample Size
  - Pseudo-Precision
  - Unrepresentative Sample
- Unsupported Assertions
  - Arguing from Ignorance
  - Unjustified Comparison
  - Unjustified Distinction
- Anecdotal Arguments
  - Correlation Implies Causation
  - Damning the Alternatives
  - Destroying the Exception
  - Destroying the Rule
  - False Dichotomy
- Omission of Key Evidence
  - Omission of Key Evidence
  - Fallacious Composition
  - Fallacious Division
  - Ignoring Available Counter-Evidence
  - Oversimplification
- Linguistic Fallacies
  - Ambiguity
  - Equivocation
  - Suppressed Quantification
  - Vacuous Explanation
  - Vagueness

Verification Approach



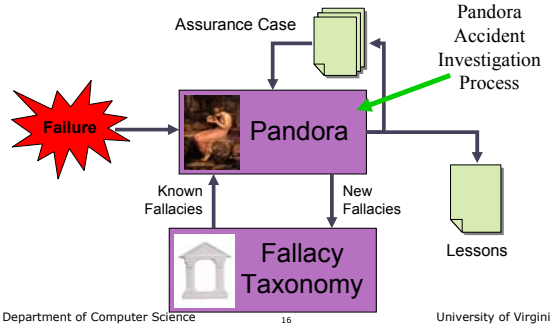
Outline

- Assurance argument fallacies
- **Accident investigation**
- Assurance based development
- Assurance based communication
- New directions in certification

Suppose Argument Is Wrong

- Despite verification of assurance case, it might still contain fallacies
- Effect might be to lead to failure:
  - Accident during operation
  - System not safe despite developers thinking it was
- If fallacy or fallacies remain, assurance case is map for finding it
- Base accident investigation on assurance case

Enhanced Assurance Case Lifecycle



Outline

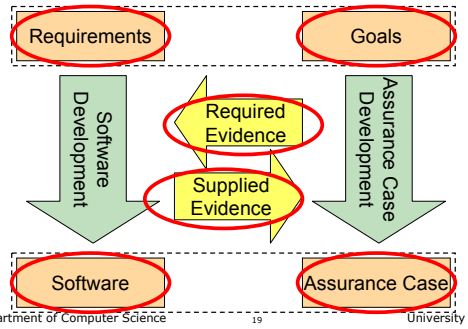
- Assurance argument fallacies
- Accident investigation
- **Assurance based development**
- Assurance based communication
- New directions in certification

Assurance Based Development

- Primary goal:

  Focus on the assurance case, not the software
- Approach:
  - Define top-level goal as "to solve the problem"
  - Develop the assurance case completely
  - This implies creation of the *evidence*
  - Part of the evidence is the software development artifacts
- Not taking this approach leaves assurance in doubt
- Traditional development is going after the ***wrong*** goal

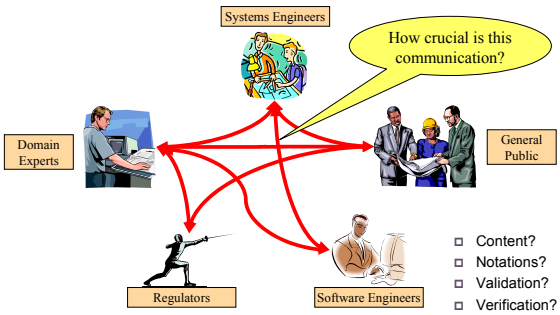
Assurance Based Development



Outline

- Assurance argument fallacies
- Accident investigation
- Assurance based development
- **Assurance based communication**
- New directions in certification

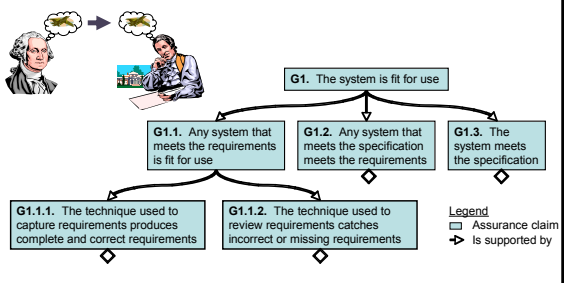
Communications Graph



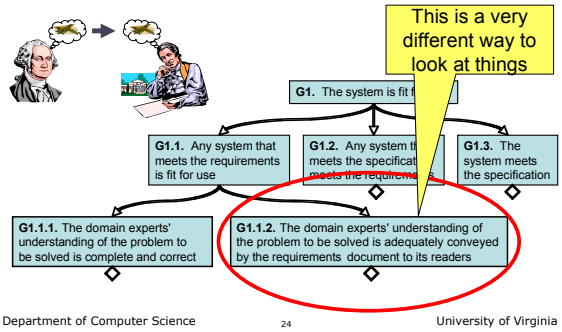
Bringing Things Together

- Make communication during development ***explicit*** in the safety/assurance case
- Establishes necessary communications quality as a *goal*
- Develop assurance/safety argument that communications goal will be met
- Incorporate appropriate techniques:
  - Formal languages, CLEAR, etc.

Requirements Argument



Better Requirements Argument



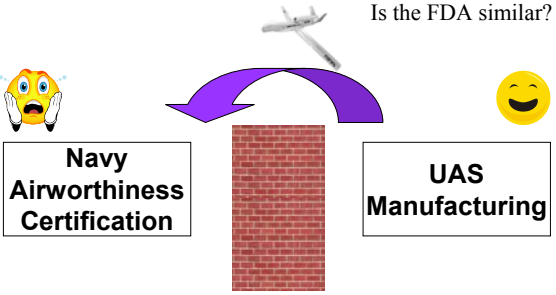
Outline

- Assurance argument fallacies
- Accident investigation
- Assurance based development
- Assurance based communication
- **New directions in certification**

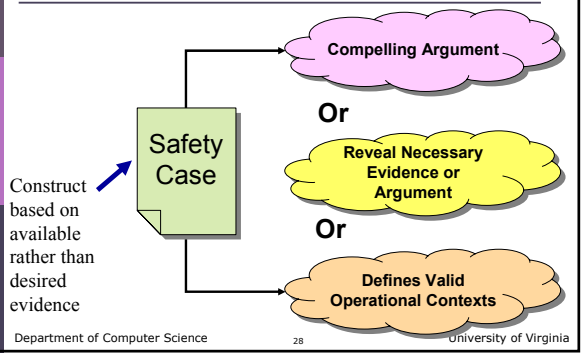
Determining Airworthiness Of Unmanned Air Systems

- Project being conducted for Navy Air Command
- Unmanned Air Systems present new challenges for Navy Air
- Approach based on safety cases
- Significant overlap with challenge faced by FDA
- Challenge:
  - Aircraft come from variety of manufacturers
  - Manufacturers do not develop comprehensive evidence
  - Need to certify because of aircraft's immediate value

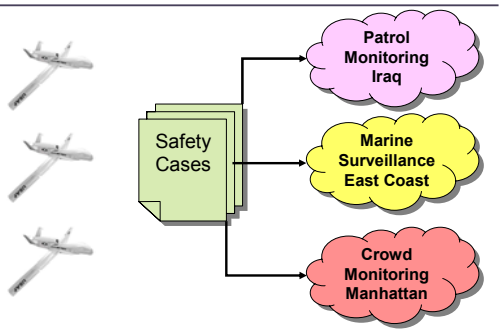
UAS Airworthiness Challenge



Strength of a Safety Case



Multiple Safety Cases For Single Aircraft



Conclusion

- Assurance of dependability is crucial
  - We need to "know" that the system will operate properly
- Presently we hope it is achieved by:
  - Ad hoc methods and experience
  - Prescribed, rigid processes
- In Assurance Based Development:
  - Assurance case is the focus, not the software
  - Development decisions influenced by impact on assurance
  - Allows a precise selection of development techniques

Contact

- E-mail address:

  knight@cs.virginia.edu
- For more information see:

  http://www.cs.virginia.edu/knight/

  http://dependability.cs.virginia.edu/