Developing Justified Confidence in the Adequacy of a Safety Case Submission

John Goodenough

Software Engineering Institute | Carnegie Mellon

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Preview: Three Points

What is a justified basis for having confidence in an assurance case?

How can a basis for confidence be used in developing a case?

What does/should a reviewer/regulator do to develop justified confidence in the conclusions of a submitted safety case?

The Safety Assurance Question for Regulators

Given a safety case (perhaps structured as an assurance case) how does a regulator decide if the safety analysis acceptably justifies its conclusion?

Answer: a confidence case for regulators

- The object of examination is the safety case submission
- The submission presents a claim, say: “The system is acceptably safe”
- The regulator examines the submission to determine whether there is a sufficient basis for accepting the claim
- Coverage is necessarily incomplete

A classic philosophical problem: determining the basis for belief in a hypothesis when it is impossible to examine every possible circumstance covered by the hypothesis

How is confidence in a hypothesis increased?

Types of Induction

Enumerative: number of confirming instances (Pascalian)

Eliminative: variety of reasons for doubt (Baconian)

Measuring support for a hypothesis/claim

- Enumerative: support increases with number of confirmations
- Eliminative: support increases with the number of excluded alternative explanations, i.e., by eliminating reasons for doubting the claim

Defeaters: reasons for doubting a claim

A Baconian Theory of AC Confidence

Confidence is the degree of belief

We grade "degree of belief" in terms of the number of eliminated defeaters (reasons for doubt)

- *i out of n* reasons for doubt *(i/n)*
- *0/n* – no confidence
- *n/n* – no remaining reasons for doubt

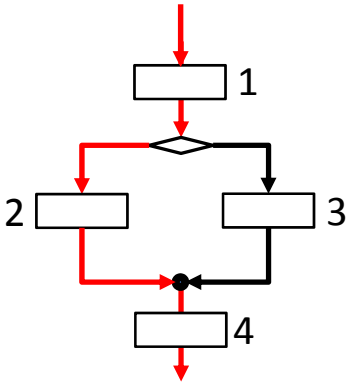
Fundamental principle: Build confidence by eliminating reasons to doubt the validity of:

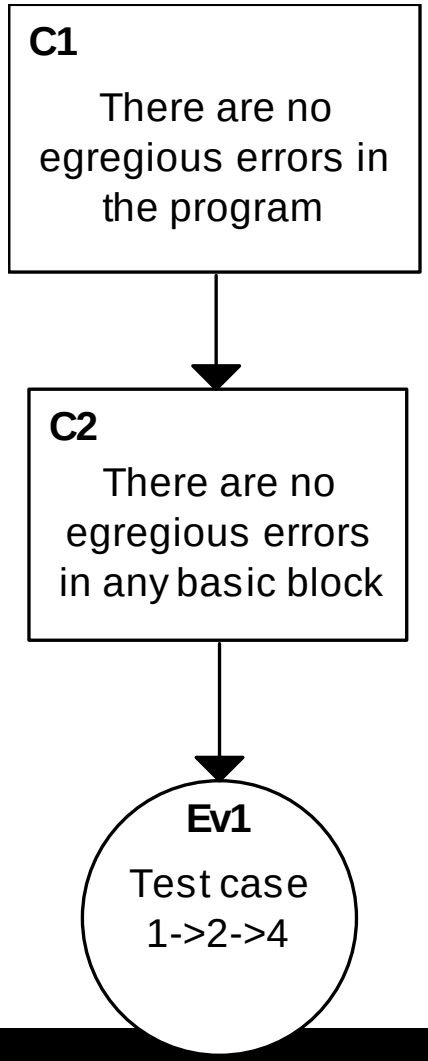
- Claims (look for counter-examples and why they can't occur)
- Evidence (look for reasons the evidence might be invalid and show those conditions do not hold)
- Inference rules (look for conditions under which the rule is not valid and why those conditions do not hold)

As more reasons for doubt are eliminated, confidence grows (eliminative induction)

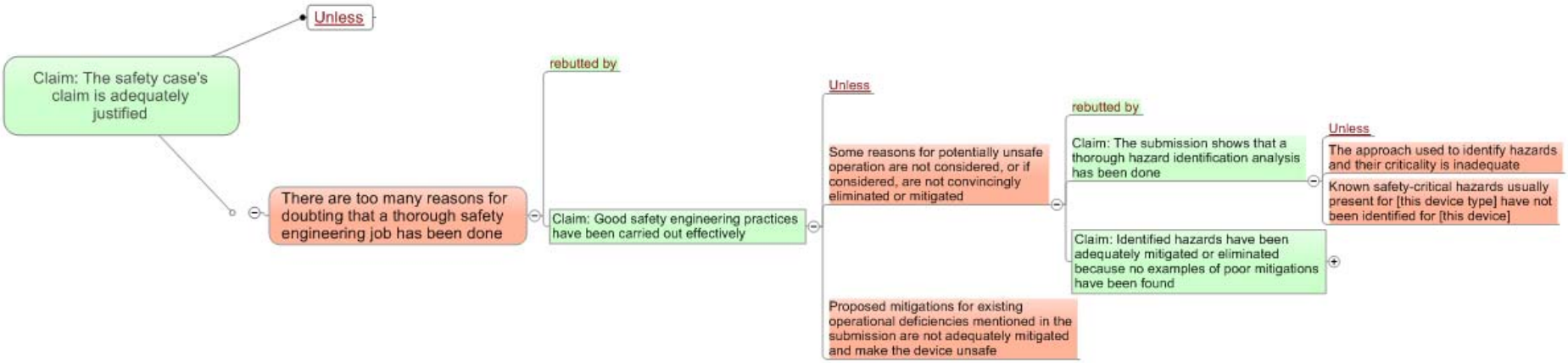
Theoretical Work on Contrived Examples

Egregious error: *Every* execution of a statement containing an egregious error will fail





A Notional Regulator Confidence Case



Possible Regulator Question (1)

Did the vendor do a competent static analysis of the code?

Why should this increase our confidence? In what claim?

- What reasons for doubt does a competent static analysis help eliminate?
  - Certain bugs that are difficult to detect by testing can be eliminated
- But how much doubt about safety is eliminated?
- Does fewer bugs mean:
  - A safer system? Are some bugs more safety critical than others?
    - Risk control mechanisms implemented in SW
- Why should the competent use of static analysis give us increased confidence?
  - It is evidence that the vendor is doing a thorough job and there are probably fewer safety-critical software errors in the device

What evidence of static analysis *competence* should be sought and why would such evidence be considered sufficient to remove doubts about competence?

Possible Regulator Question (2)

Did the submitter do a good job vetting user requirements, e.g., are they "complete" and consistent?

Why should this increase our confidence? What reasons for doubt does a positive answer eliminate?

- The system's response to unspecified user behavior could be unsafe
- What kind of doubt does the absence of such analysis justifiably raise in a reviewer's mind

Given a claim that user requirements have been vetted, what would be good reasons for doubt that the vetting was competent and sufficient?

Summary

For a reviewer to have confidence in a submission, what kind of evidential support should be sought from the submission, and on what basis does the regulator decide when it is enough?

- Kind of evidential support
  - Information that eliminates defeaters in the reviewer's confidence case
- When to stop
  - When remaining defeaters are not a concern

Constructing a case

- For each claim, identify what would be counter-examples or would raise doubts and determine how to show they cannot occur
- For each item of evidence, identify what would make the evidence less credible and determine how to eliminate those conditions
- For each inference rule, identify the conditions that make the rule potentially inconclusive, e.g.
  - "if all hazards are eliminated, the system is safe" holds only if you are sure that all hazards have been identified

Contact Information

John B. Goodenough

SEI Fellow, Retired

Research, Technology, and System Solutions

Telephone: +1 412-390-4043

Email: jbg@sei.cmu.edu

U.S. Mail

Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Web

www.sei.cmu.edu

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257