Developing Sufficient (Justified) Confidence in Claims about a System

John B. Goodenough

Charles B. Weinstock

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-0418

Topics

A brief overview of “confidence”

The Method of Doubts – A basis for “confidence”

“Confidence”: A deeper dive

Having Confidence

What *is* confidence

- e.g., what does “80% confidence” mean?
  - Probability of operational failure or accident (e.g., P(Failure) < 20%)?
    - On demand – 80% of the time you make a demand, it succeeds?
    - Over some period – a mission of 100 hours is 80% likely to succeed?
  - Combination of probability of failure and consequence of a failure?
    - Safety integrity levels
    - Residual risk
  - Degree of belief that a claim holds?
    - Absence of doubt (80% of doubts eliminated)
    - Can vary among different holders of the belief

Having Confidence

Confidence changes over time

- As more is known, e.g.,
  - While developing a system
  - While investigating a system (building a case)
  - As you discover counterevidence
- Increases as uncertainty decreases (subjective logic)
- Degrades with time
  - As assumptions are invalidated (e.g., system environment or usage changes)
  - As confidence in evidence decays (e.g., do tests still pass?)

What is “Sufficient” Confidence?

A degree of belief that makes you comfortable acting on the validity of a claim

- We don’t want to regret actions based on our belief
- “Sufficient” if you can act as if a claim is true without having unacceptable consequences
  - Depends on consequences if a claim is false and likelihood of falsity
  - Is partly a function of your belief in a claim
  - The bar is higher if consequences are “bad”

Possible metric (of confidence)

- Number (or significance) of remaining doubts
- Tells us how much work remains before we will have “sufficient” confidence

What is “Justified” Confidence?

A [valid | believable | agreed] explanation for your belief in a claim’s truth

Justified confidence can be any value between 0 and certainty!

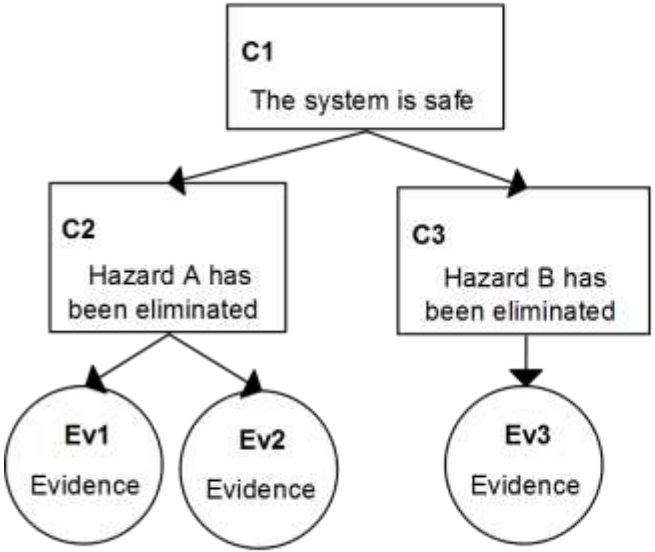
Overview

A brief overview of “confidence”

The Method of Doubts – A basis for “confidence”

“Confidence”: A deeper dive

A Notional Assurance Case

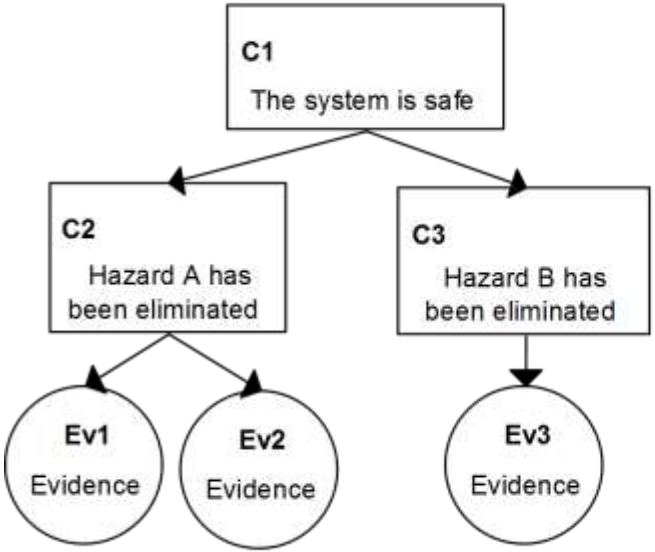


The Problem

Given the evidence, how confident should we be in the claim C1? Why?

What does it mean to have confidence in the claim?

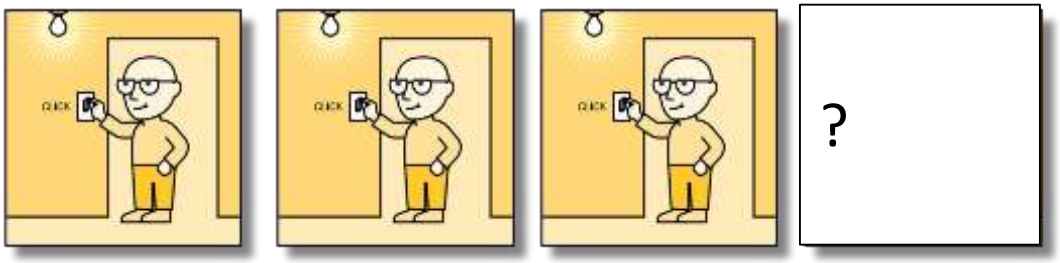
What could be done to improve confidence? Why?



The Basis for Confidence in a Claim

Use Enumerative Induction

- Support increases as **confirming instances** are found



The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - Switch not connected to light
  - No power
  - Dead light bulb

The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - Switch not connected to light
  - No power
  - Dead light bulb

The Basis for Confidence in a Claim

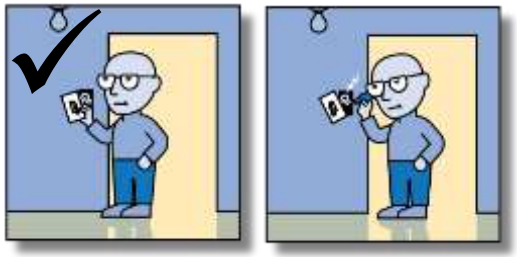
Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~
  - No power
  - Dead light bulb

The Basis for Confidence in a Claim

Use **Eliminative** Induction

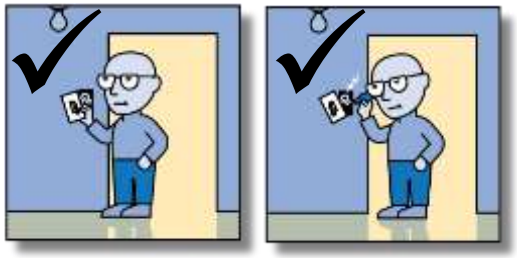
- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~
  - No power
  - Dead light bulb



The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~
  - ~~No power~~
  - Dead light bulb



The Basis for Confidence in a Claim

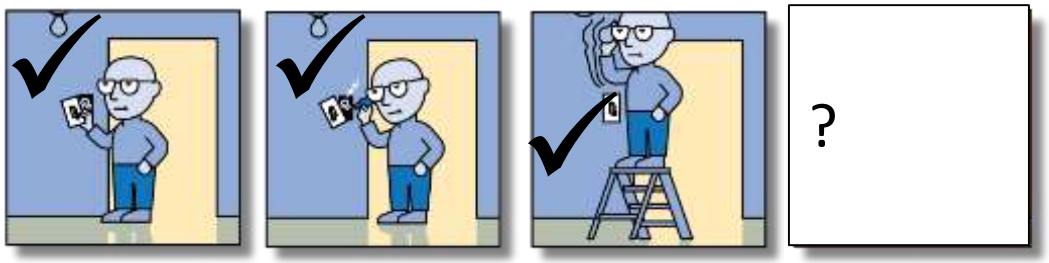
Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~
  - ~~No power~~
  - Dead light bulb

The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~
  - ~~No power~~
  - ~~Dead light bulb~~



The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - ~~Switch not connected to light~~ – *3/3* (complete confidence)
  - ~~No power~~
  - ~~Dead light bulb~~

The Basis for Confidence in a Claim

Use **Eliminative** Induction

- Support increases as **reasons for doubt** are eliminated
  - Switch not connected to light – $3/3$ (complete confidence)
  - No power – $0/3$ (no confidence)
  - Dead light bulb – $2/3$ (partial confidence)

The Basis for Confidence in a Claim

Use **Eliminative** Induction

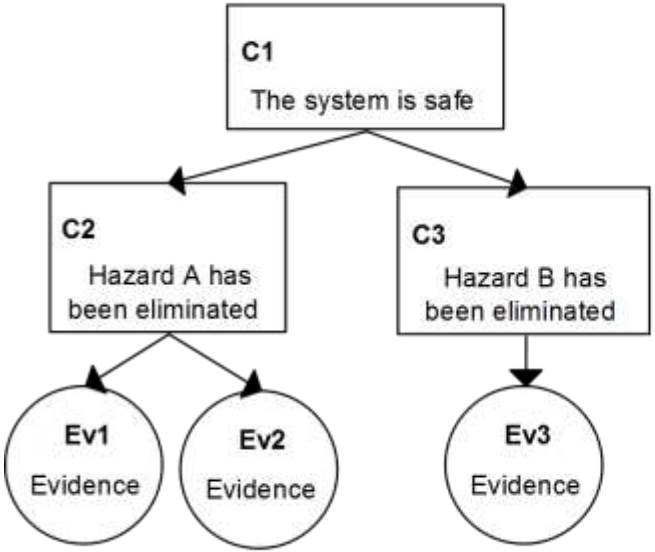
- Support increases as **reasons for doubt** are eliminated
  - Switch not connected to light – *3/3* (complete confidence)
  - ~~No power~~ – *0/3* (no confidence)
  - ~~Dead light bulb~~ – *2/3* (partial confidence)

The Problem

How confident in C1? Why? (Number of uneliminated doubts)

What does it mean to have confidence? (To have no doubt)

What could be done to improve confidence? Why? (Elim. more doubts)



The Method of Doubts

A form of structured argumentation incorporating concepts from

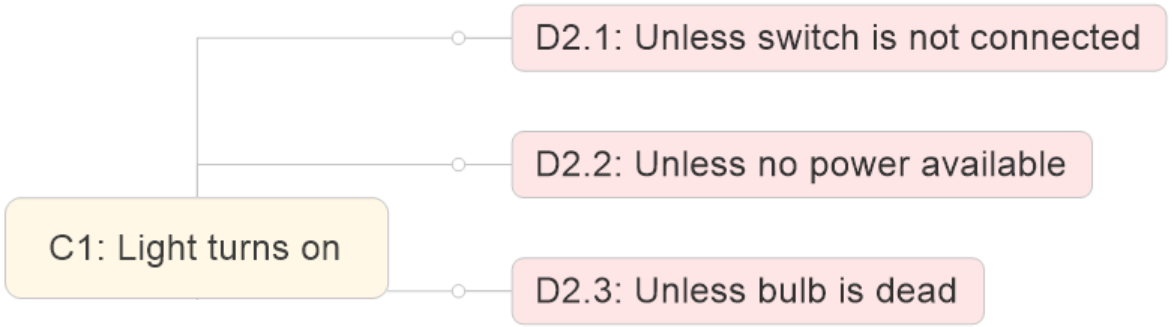
- Assurance cases
- Eliminative induction
- Defeasible reasoning

The Method of Doubts uses an eliminative argument to show the basis for confidence in an argument's conclusion

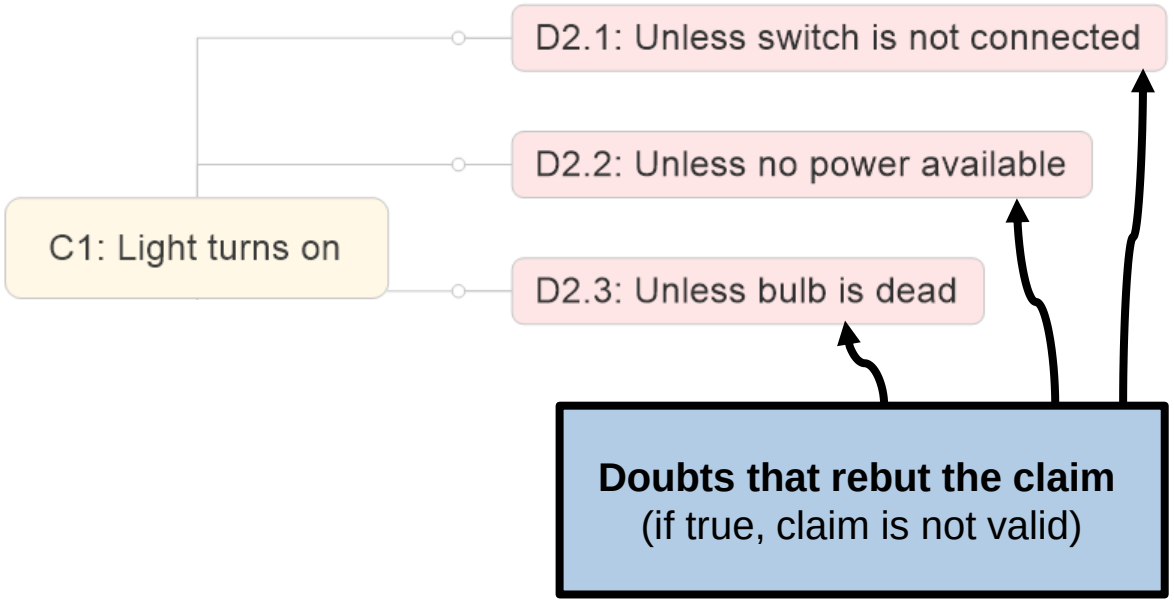
An eliminative argument is visualized in a *confidence map*, which shows reasons for doubt graphically.

It's a reframing of an assurance argument to make doubts explicit.

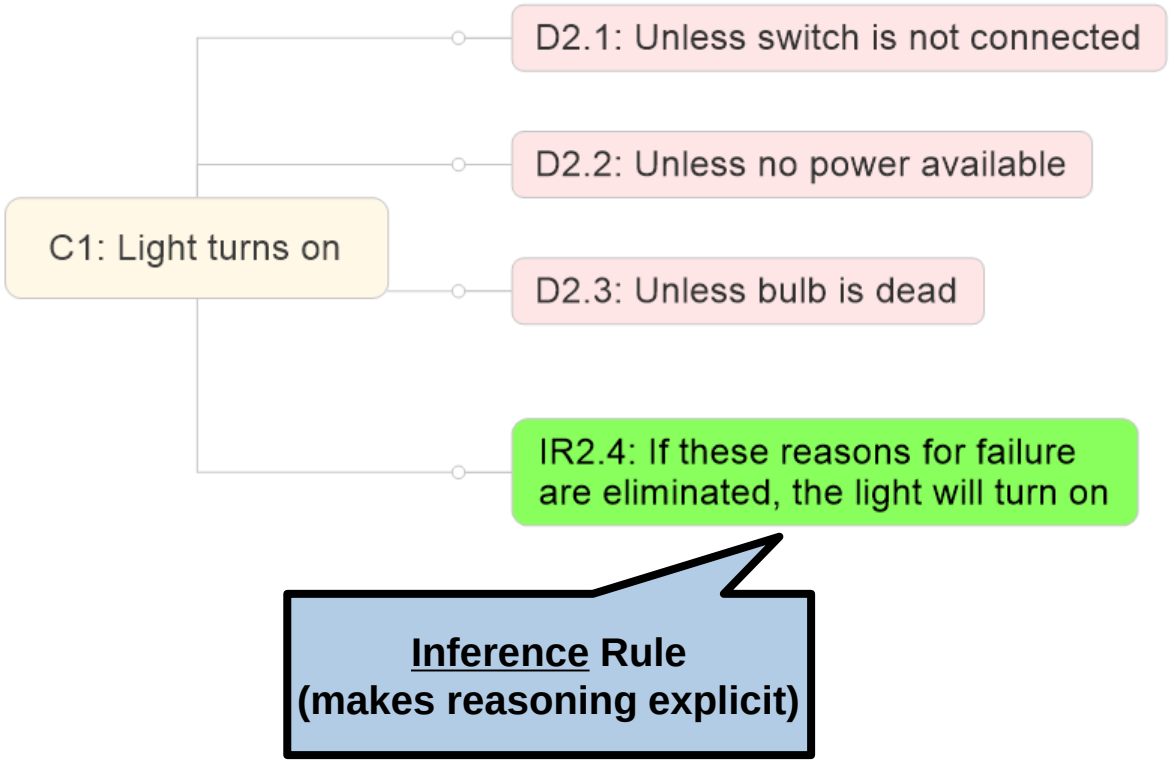
A Confidence Map



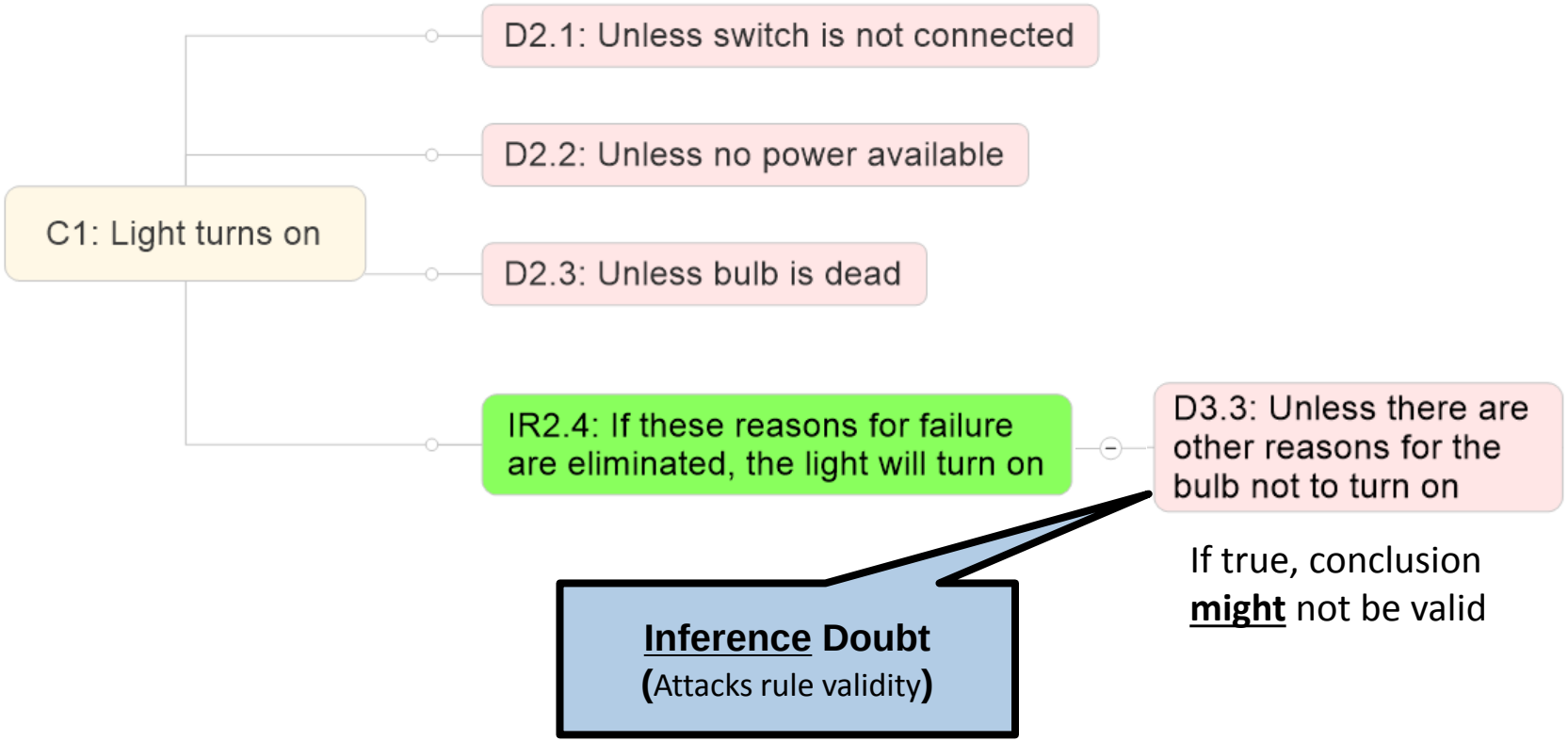
A Confidence Map



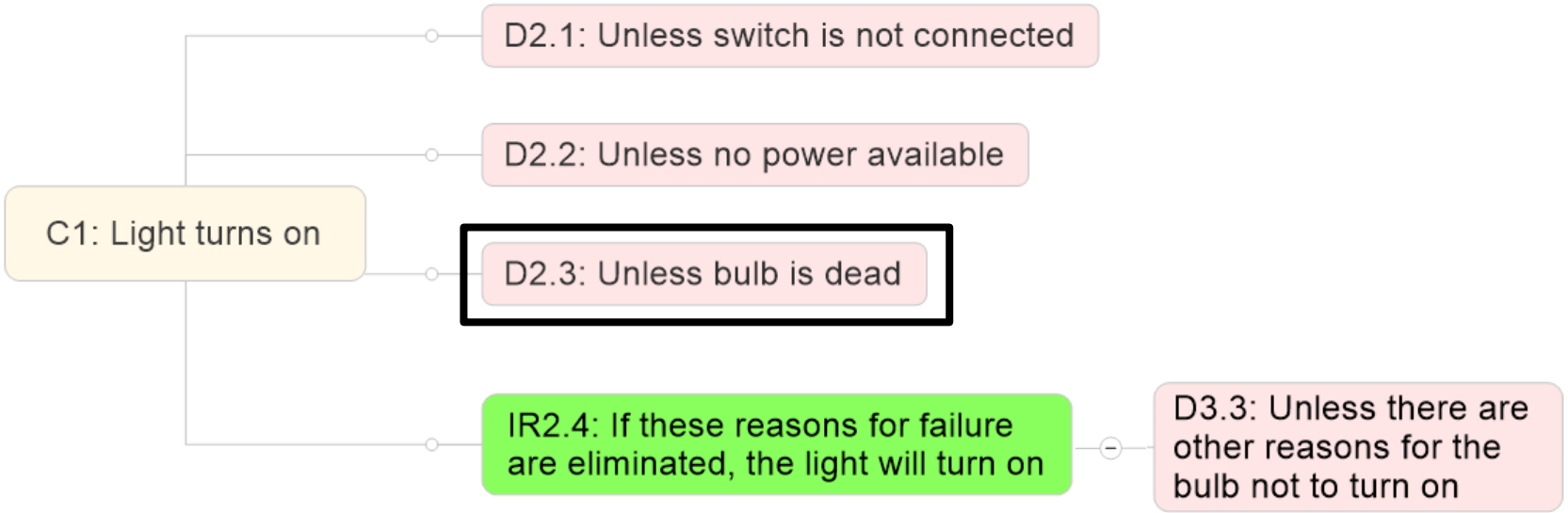
A Confidence Map

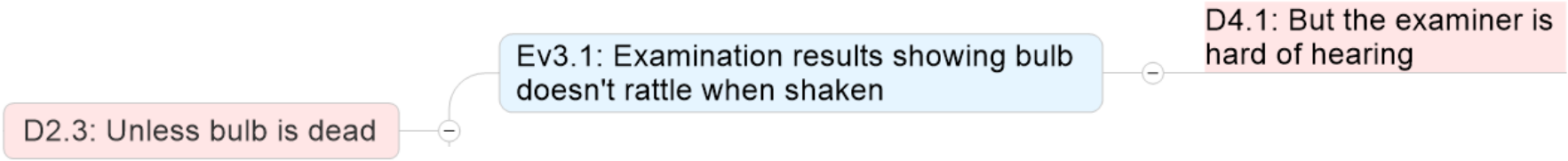


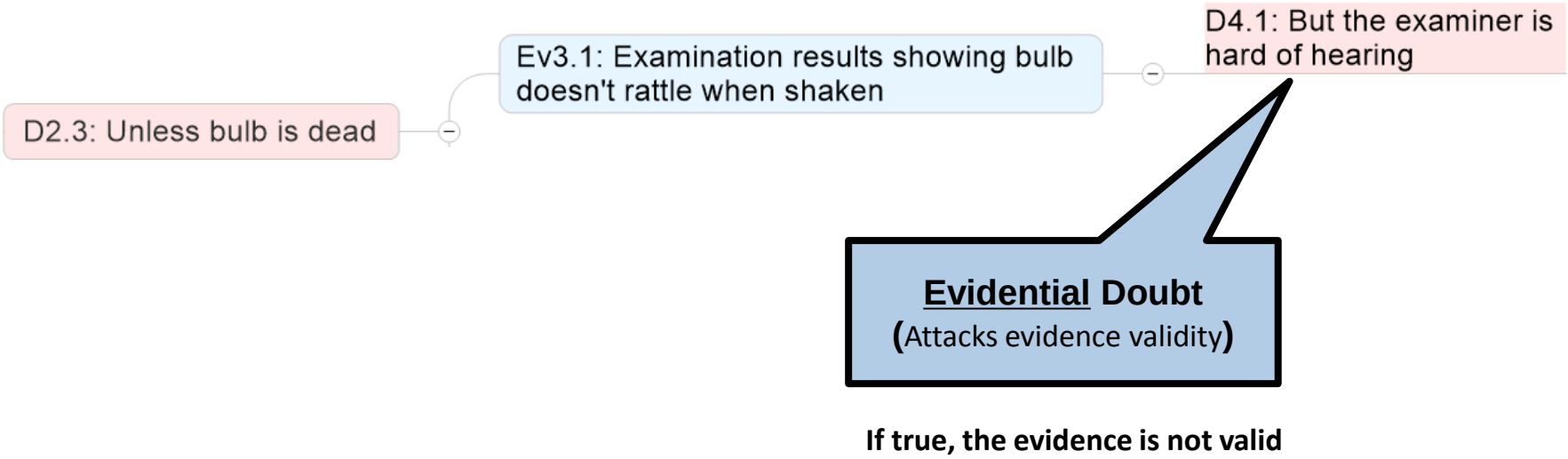
A Confidence Map



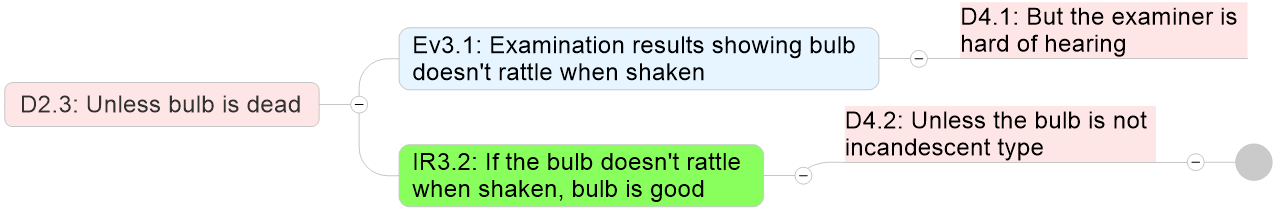
A Confidence Map

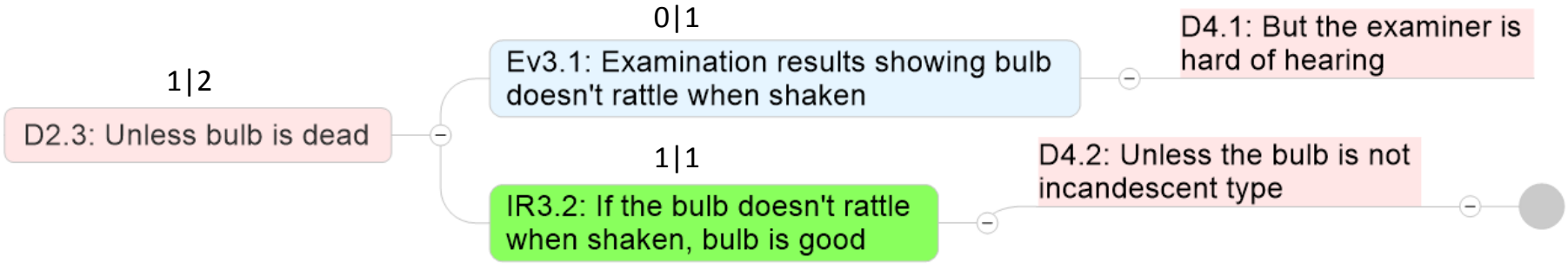


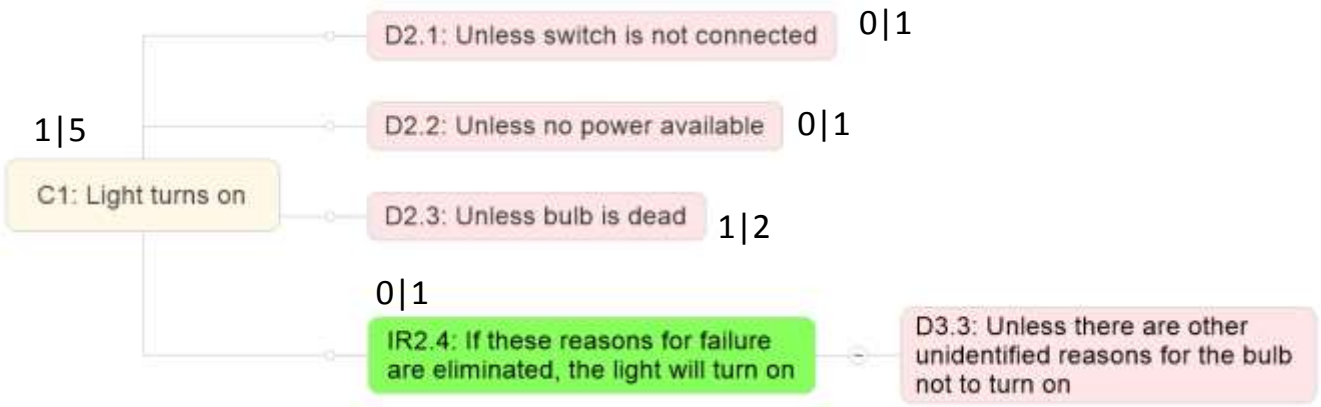




If true, the evidence is not valid







Sources of Doubt

Finding doubts

- Doubts that attack claim — why claim may be **false**
- Doubts that attack evidence — why evidence may be **compromised**
- Doubts that attack the inference — premise ok; **conclusion uncertain**

Overview

A brief overview of “confidence”

The Method of Doubts – A basis for “confidence”

“Confidence”: A deeper dive

A Deeper Dive

What information gives us confidence?

What information gives us SUFFICIENT confidence?

What information gives us JUSTIFIED confidence?

What can we do with a measure of confidence?

What Information Gives Us Confidence?

All the tests run successfully?

- Only if we know what doubts are eliminated by the test results
- Only if we know why the tests are valid (for the purpose of eliminating some doubt)
- If some tests are not run (e.g., too expensive), what doubts may remain?

4 out of 5 assessors agree that a system claim is likely to hold?

- A weak form of evidence linked by a weak inference rule

The soundness and completeness of a confidence argument?

- Not entirely clear how to integrate incompletely eliminated doubts

What Information Gives Us SUFFICIENT Confidence?

Lack of doubt that the system will misbehave

- One has to eliminate a sufficient number of significant defeaters
- Significant defeaters, when true, lead to significant negative outcomes for users of a system

A notion of which defeaters are significant and confidence that they have been eliminated

- Recursive!

The number, status, and significance of defeaters provides a function relevant to confidence

What Information Gives Us JUSTIFIED Confidence?

Arguments and evidence presented to show when (and to what extent) doubts are eliminated

What Can We Do With a Measure of Confidence?

Make a management decision (i.e., decide which unmitigated doubts can be tolerated)

- Release a version
- Assert that a system is X (safe, secure, …)

Make a development decision on resource allocation

- Where to invest resources (on eliminating doubts contributing most to lack of confidence)
- Choose actions that reduce risk or significance of failure (e.g., change claims)
- Export responsibility for eliminating certain doubts (e.g., increase effectiveness of user training)

Convince a regulator that a system is X (safe, secure, …)

What we want to do affects what measure is appropriate

Why Use the Method of Doubts?

The different kinds of doubts stimulate thought about what might lead to a loss of confidence

- In short, it helps in developing an assurance argument
- Reduces confirmation bias

The confidence map is a tree that can be decorated with various confidence calculations

- It is a framework for a confidence calculus

Thinking in terms of identifying and eliminating doubts gives a concrete mental model for understanding why you should be confident

Is a framework for thinking about much of what is already done today

It has been proven to have practical value in at least one known commercial use

QNX Experience

"QNX prepared Assurance Cases for its operating system product in 2010, 2012, 2013, 2014, 2015, 2016, in each using both GSN and Bayesian Belief Network. … In 2018, [used Method of Doubts].

Without the need for a Bayesian Belief Network, this latest Assurance Case uncovered more than twenty previously missed problems: some being procedural and some being technical. … [T]hirteen Concession Requests [were] submitted to the certification body (TŰV Rheinland). These Concession Requests effectively say, 'We have identified a problem with our adherence to paragraph X of ISO 26262, but cannot fix it immediately.' …

With the new approach, QNX found that it was not necessary to prepare two Assurance Cases: one using GSN to satisfy an auditor and one using BBNs to satisfy internal Safety Engineers."

Hobbs, Chris. *Experience with Assurance Case Preparation*, Blackberry QNX, December, 2018.

Success Stories

- QNX (BlackBerry): identified more than 20 problems in a previously assured and certified product. Made 13 Concession Requests to the certification authority. Adopted as their standard approach
- FDA: developed argumentation requirements to be placed on medical device manufacturer submissions
- NASA: constructed a demo likely to persuade their management
- FCS: provided an early indication of whether a milestone would be met
- SEI: answered questions regarding SEI value to the DoD; provided evidence to ground LSI/LENS portfolio decisions
- FAA: determined when a system might be too complex to certify
- NS: highlighted areas of focus for to help them meet a Federally-mandated deadline for the deployment of PTC
- ATEC: informed cybersecurity risks of using the cloud
- HBI: identified export control risks

References

Short paper covering the key ideas: Goodenough, J.B., Weinstock, C.B., Klein, A.Z., “Eliminative induction: A basis for arguing system confidence”, Proc. of 35th International Conference on Software Engineering, pp. 1161-1164, (2013).

Comprehensive report: Goodenough, J., Weinstock, C, and Klein, A. “Eliminative Argumentation: A Basis for Arguing Confidence in System Properties,” CMU/SEI-2015-TR-005, Software Engineering Institute, Carnegie Mellon University, 2015, https://doi.org/10.1184/R1/6573413.v1

Contact Information

John B. Goodenough
SEI Fellow
Telephone: +1 412-390-4043
Email: jbg@sei.cmu.edu

Charles B. Weinstock
Principal Researcher
Telephone: +1 412-268-7719
Email: weinstock@sei.cmu.edu

U.S. Mail
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA