Building Confidence Incrementally

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.

DM22-1022

Building Confidence in an Interface Device

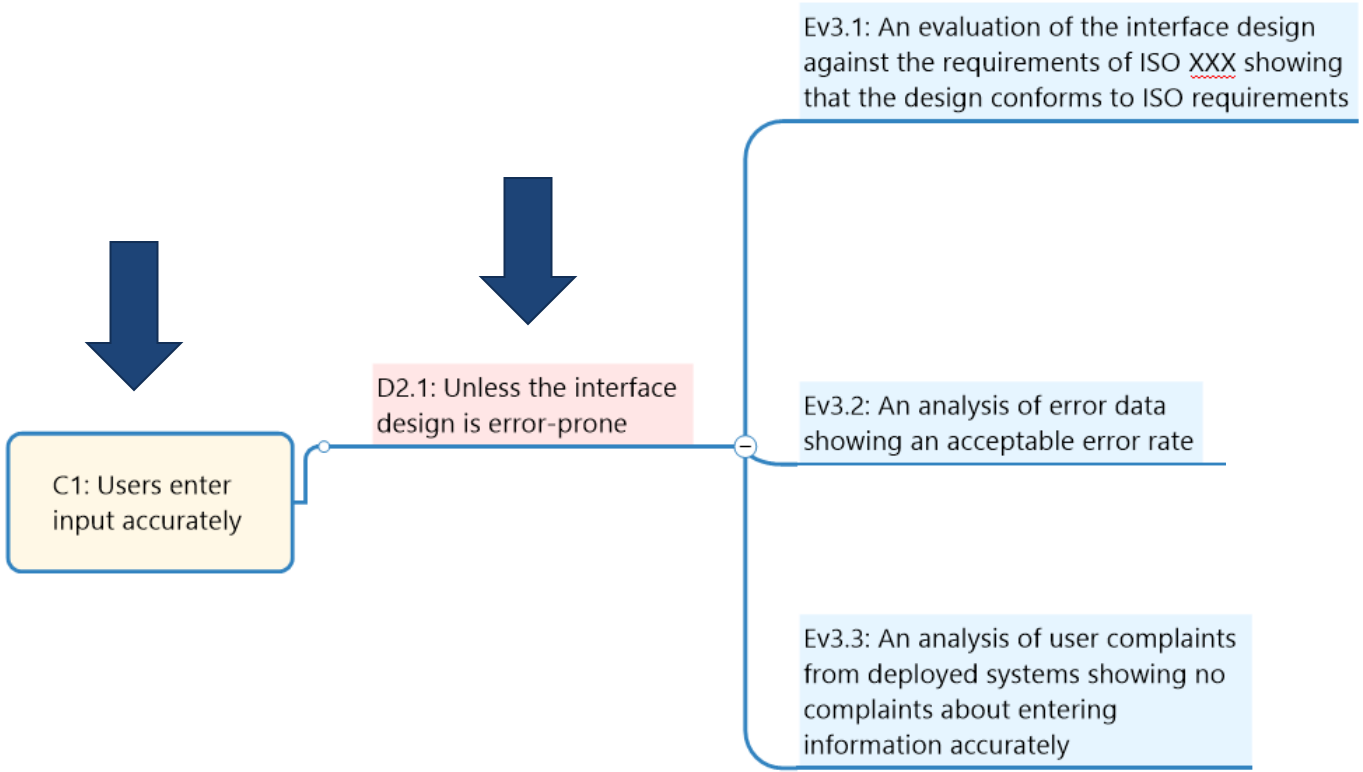
When designing a new interface device such as this one, there is a requirement that the user error rate be acceptably low.

Building Confidence in an Interface Device

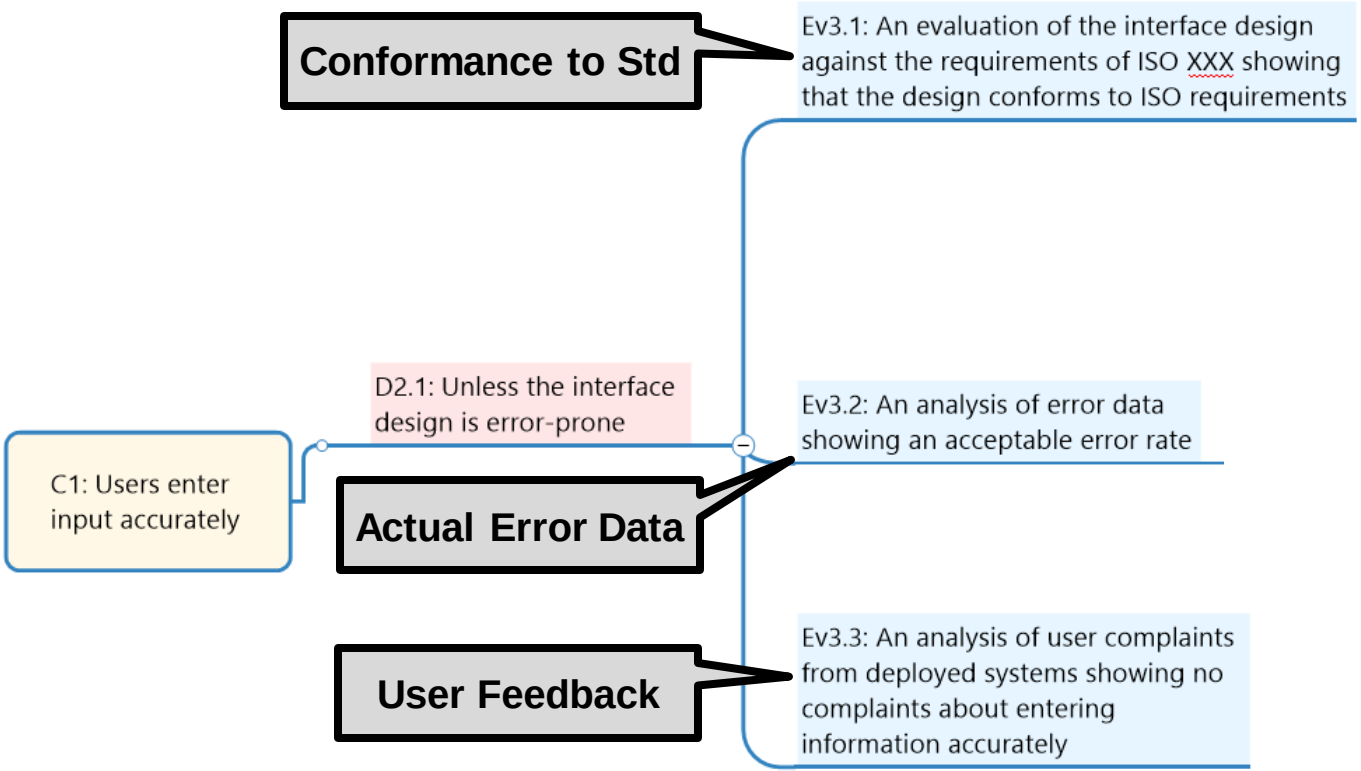
When designing a new interface device such as this one, there is a requirement that the user error rate be acceptably low.

How might assurance be developed incrementally as the design and implementation evolve?

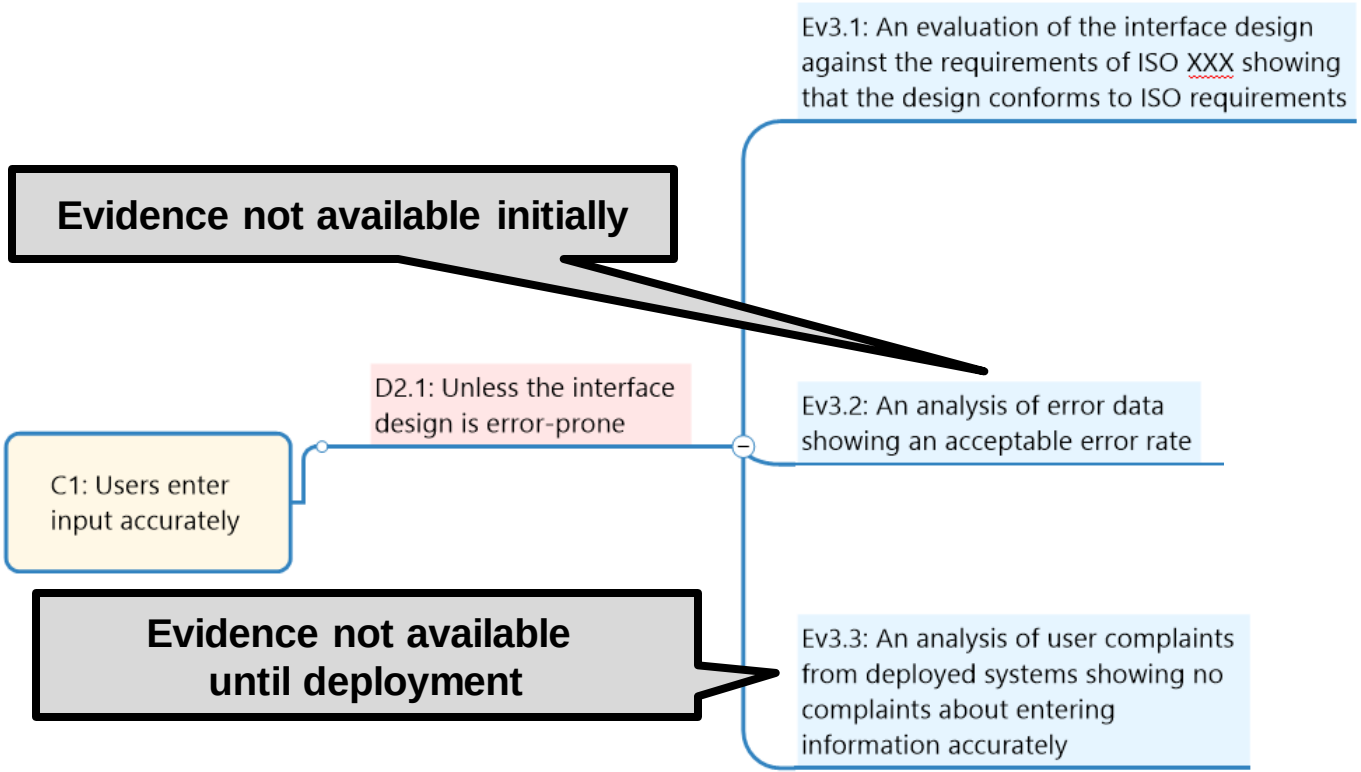
Building Confidence in an Interface Device



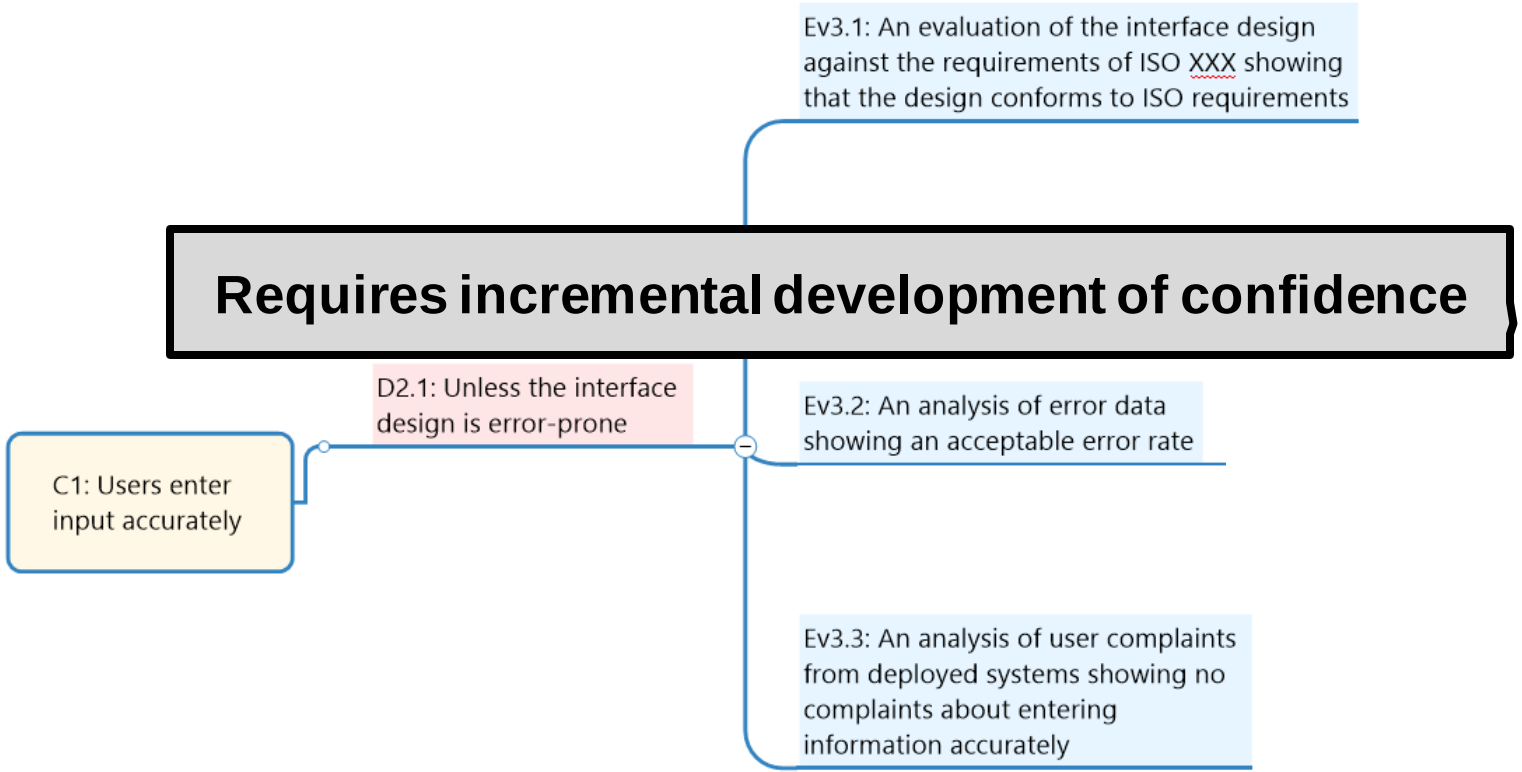
Building Confidence in an Interface Device



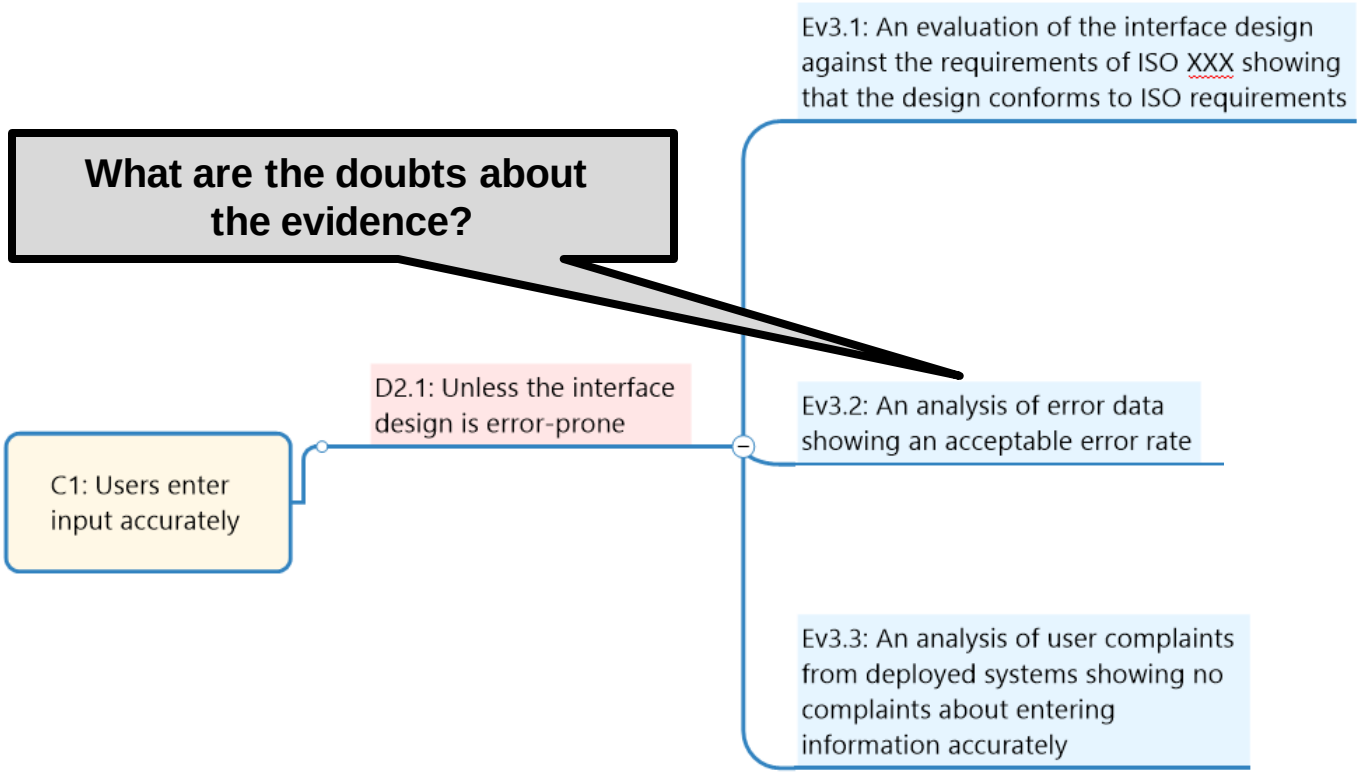
Building Confidence in an Interface Device



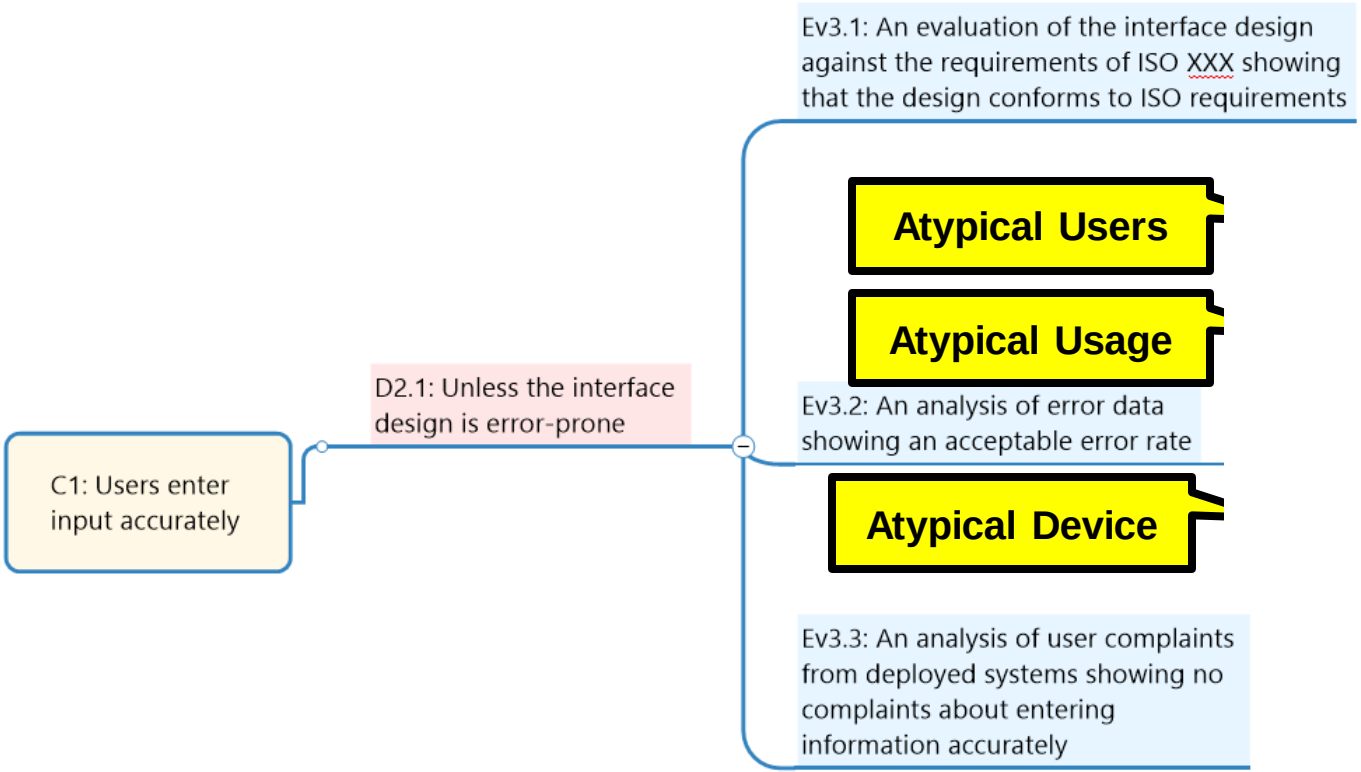
Building Confidence in an Interface Device



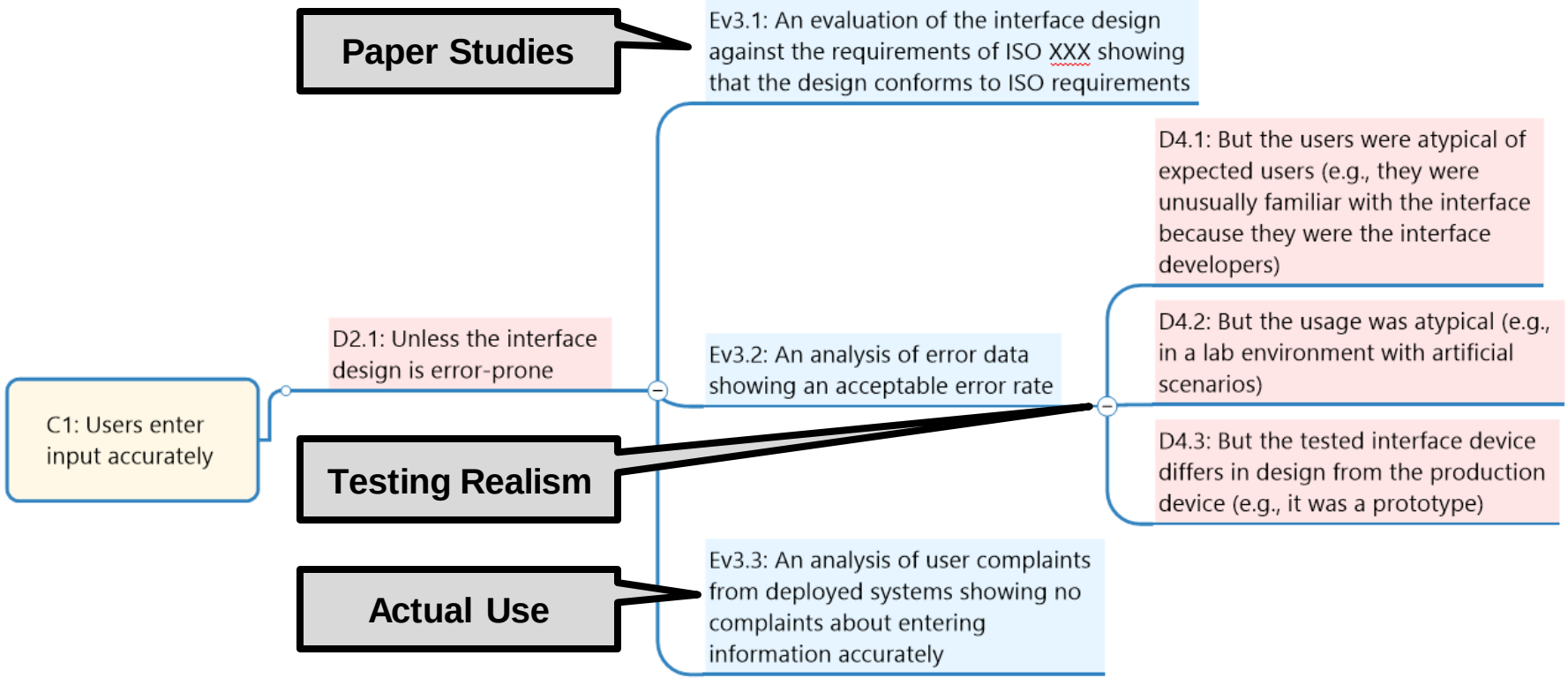
Building Confidence in an Interface Device



Building Confidence in an Interface Device



Building Confidence in an Interface Device



Incremental Confidence

As more information becomes available, confidence can increase

The AC can outline the lifecycle strategy for building (and maintaining) confidence

- Including the increase in doubt as time goes by (is the error rate maintained?)

Confidence in **evidence** plays a significant role in incremental confidence

How much confidence is needed to move to a next development stage?

- Depends on the significance of the remaining doubts
- The ability to gather evidence that eliminates the doubts
- How to measure is unclear (i.e., how much residual doubt is acceptable at some stage
  - Counting uneliminated **significant** doubts is a possibly pragmatic approach

What Information Gives Us SUFFICIENT Confidence?

Significant doubts, if valid, would lead to significant negative outcomes

- When actions are taken based on a belief that a claim is valid

Sufficient confidence is, in part, a function of

- The number, status, and significance of uneliminated doubts
- One has to eliminate a sufficient number of significant doubts
  - But which are significant?
  - How completely are they eliminated?

What is Confidence?

Confidence: the degree of belief that a claim holds

- Possible Measures:
  - Absence of doubt (80% of doubts eliminated)?
  - 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?
  - Some combination of probability of failure and consequence of a failure?
    - Safety integrity levels
    - Residual risk
- Can vary among different holders of the belief
- What does it mean to be more “highly assured”?

What is Confidence?

Confidence changes over time

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

What is “Sufficient” Confidence?

“Sufficient” if the consequences of acting as if a claim is true are acceptable

- Release a system
- Approve a design
- Stop perfecting the evidence

The bar is higher if potential consequences are “bad”

Interesting Questions about Confidence

How does a "defense in depth" design strategy impact confidence?

- How do you show that additional confidence created by secondary defense is worthwhile?
  - What doubts does such a strategy eliminate?
  - Why do redundant checks eliminate doubts (that have already been eliminated)?

If we modify a system by adding an electric generator to mitigate the risk of a power outage, do we need to modify the claim to explain what we have increased confidence in?

- E.g., have more confidence in an increased MTF measure?
- Before adding the generator, could have high confidence in a 3 9's claim and hardly any in a 5 9's claim

What about when adding recovery actions to mitigate the damage caused by an intrusion?

- This must increase the confidence in some modified claim about the availability of a system capability. Anything else?

What does it mean to be more "highly assured"

- Fewer uneliminated doubts?
- More doubts identified and eliminated?
- More stringent claim in which to have confidence?

Contact Information

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

Charles B. Weinstock
Principal Researcher
Telephone: +1 412-298-9747
Email: weinstock@sei.cmu.edu

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