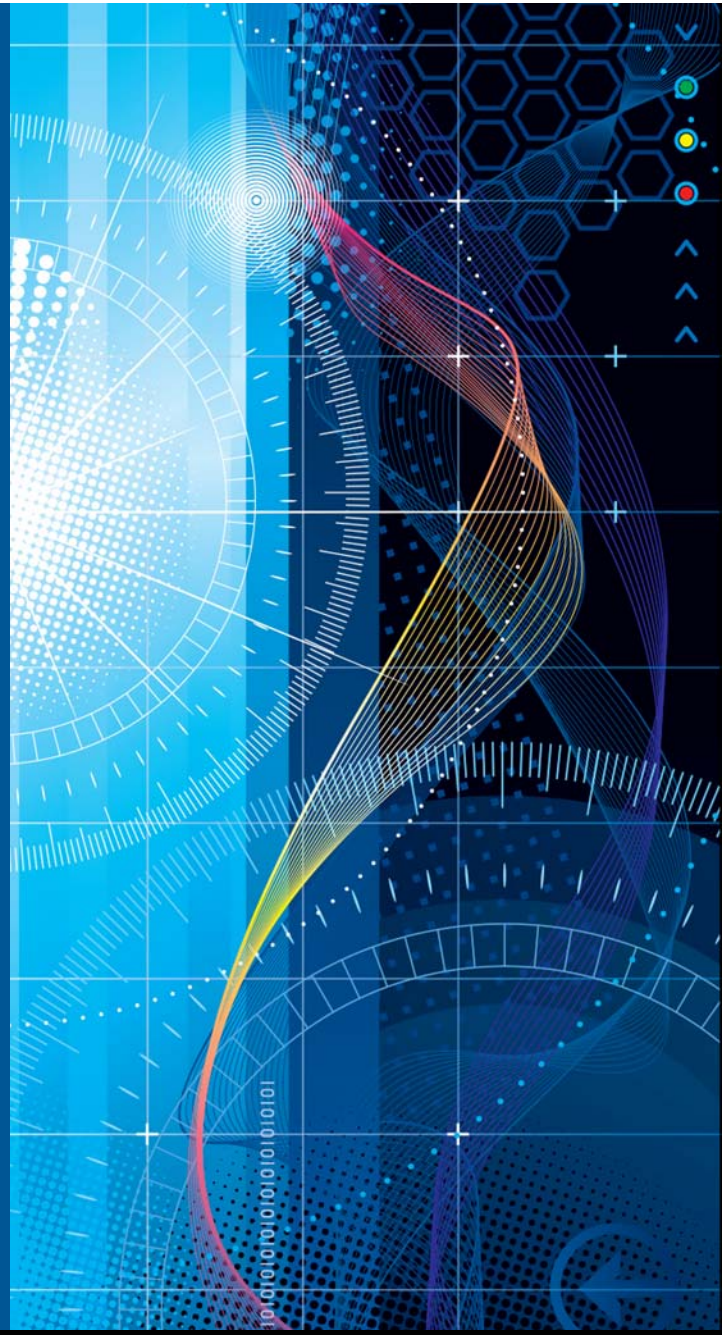
Using a Perfect Argument in an Imperfect World

John B. Goodenough

Charles B Weinstock

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



© 2015 Carnegie Mellon University

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

Copyright 2015 ACM

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.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM-0002604

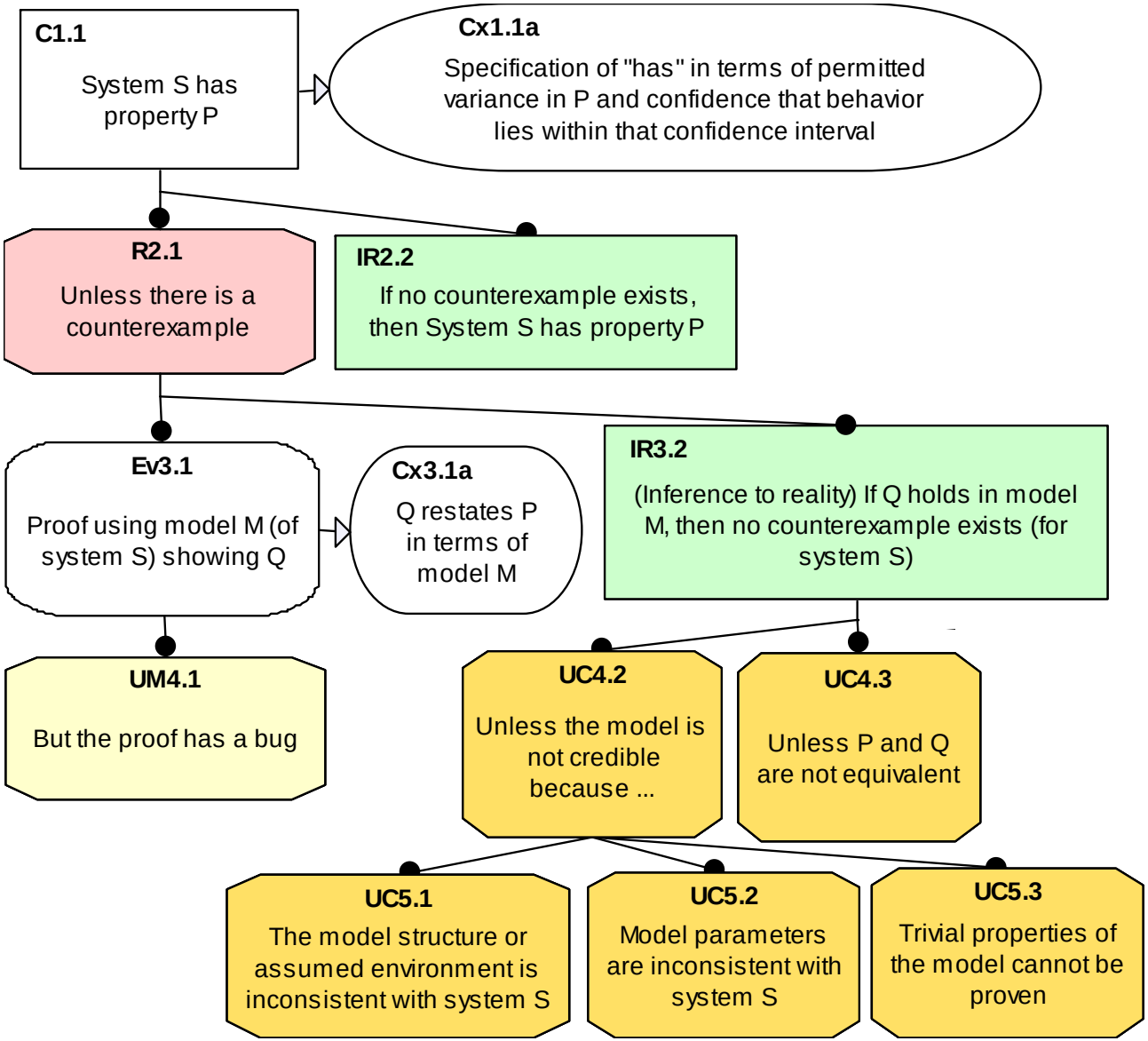
Overview

The role of proof in an assurance case

- Use *eliminative argumentation*
  - Doubts about validity of claims
  - Doubts about validity of evidence
  - Doubts about validity of inferences
- As doubts are eliminated, confidence increases
  - Schema for use of proof
  - Trivial example
  - More realistic example

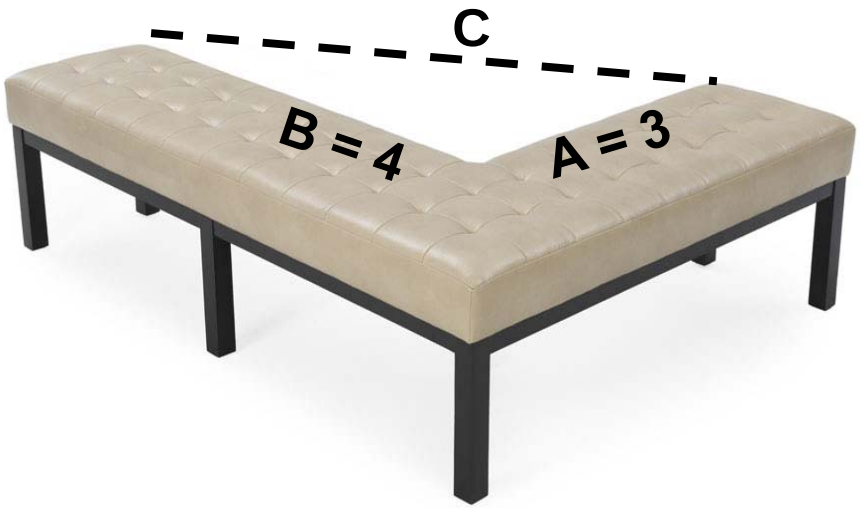
© 2015 Carnegie Mellon University

Schema for Use of Proof in a Case



© 2015 Carnegie Mellon University

Triangle Example



© 2015 Carnegie Mellon University

Triangle Example

C1.1

In physical triangle ABC (system S), C = 5

Cx1.1a

C = 5 means C lies within 0.02 of 5 with 99% confidence

R2.1

Unless when A = 3 and B = 4, C is not to equal to 5

IR2.2

If there is no possibility that C /= 5, then C = 5

Cx3.1a

B' = 4

C'

A' = 3

Ev3.1

Proof using model M showing C' = sqrt(A'*A' + B'*B'), and so C' must equal 5

IR3.2

(Inference to reality) If C' = 5 in the model then C must equal 5 in system S

UC4.1

Unless the model is not credible because ...

UC4.2

Unless C'=5 is not equivalent to saying C=5

UC5.1

The physical triangle does not lie in a plane

UC5.2

The actual values of A, B, and angle AB are too different from those in model M

UC5.3

Angles A'C' and B'C' do not sum to 90 degrees

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

Calculating Confidence

$A = 3 \pm 0.02$ (with 99% confidence)

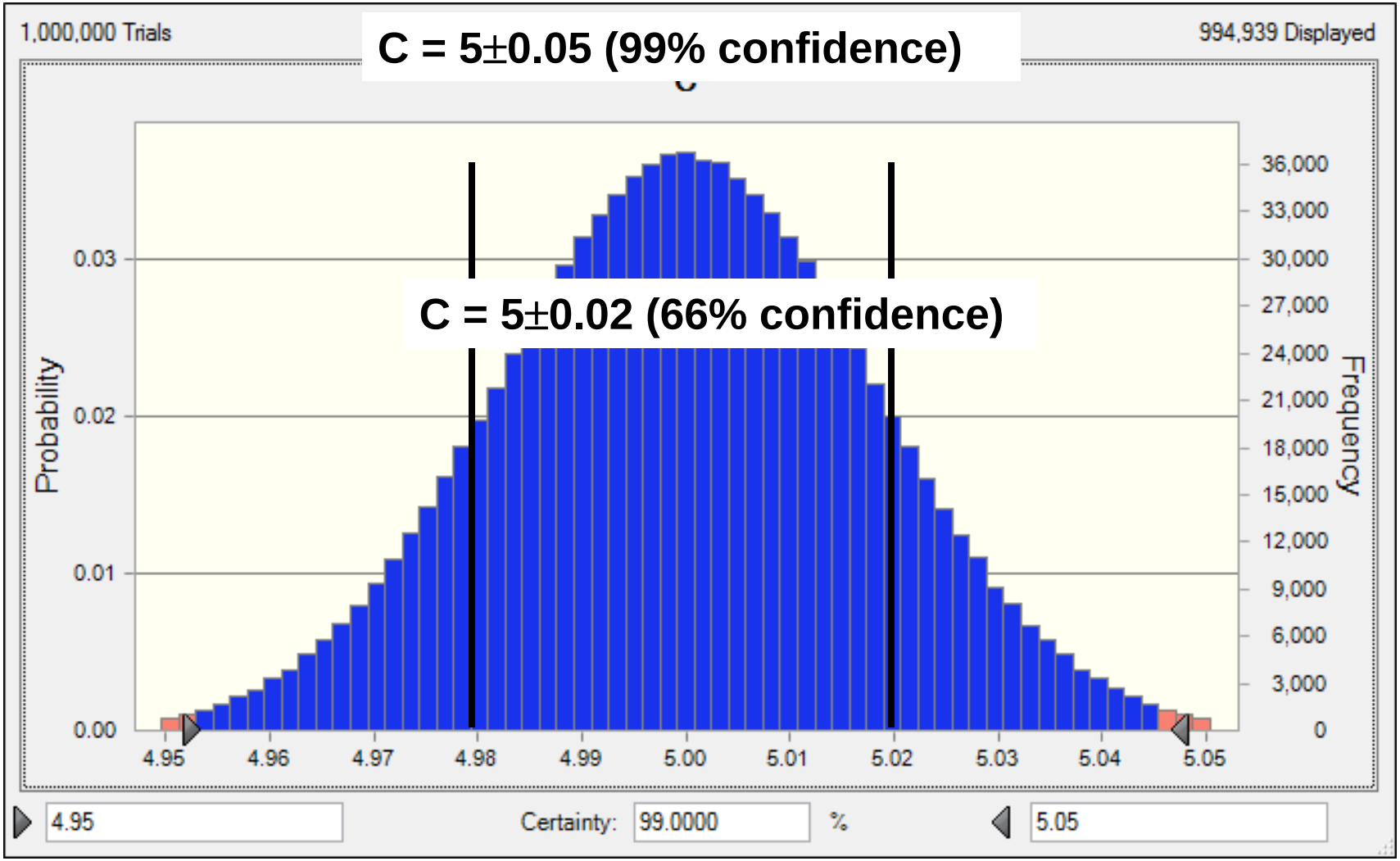
$B = 4 \pm 0.02$ (with 99% confidence)

$\alpha = 90° \pm 1.0°$ (with 99% confidence)

$C = sqrt\ (A^2 + B^2 - 2AB\cos(\alpha))$

© 2015 Carnegie Mellon University

Calculating Confidence



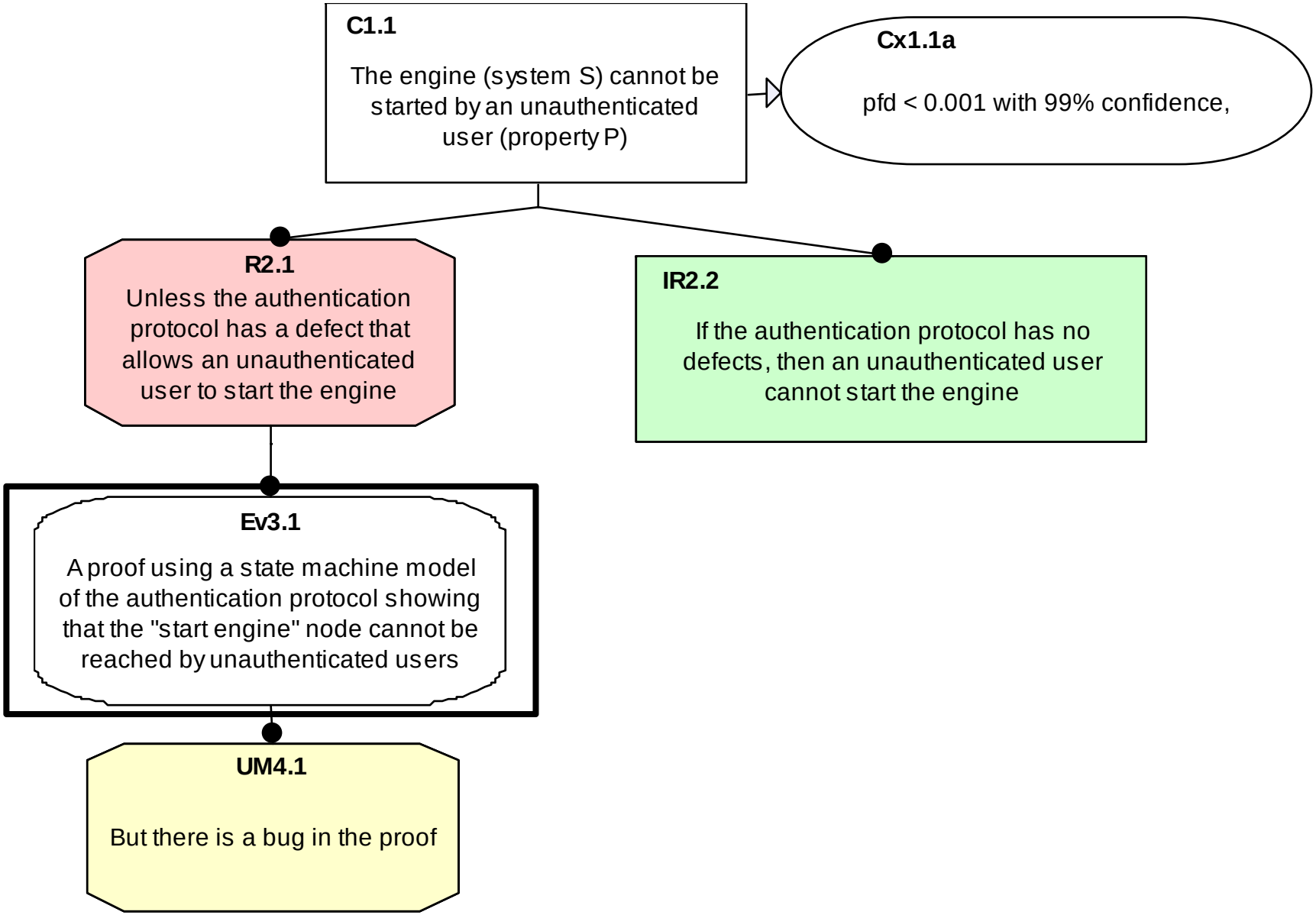
© 2015 Carnegie Mellon University

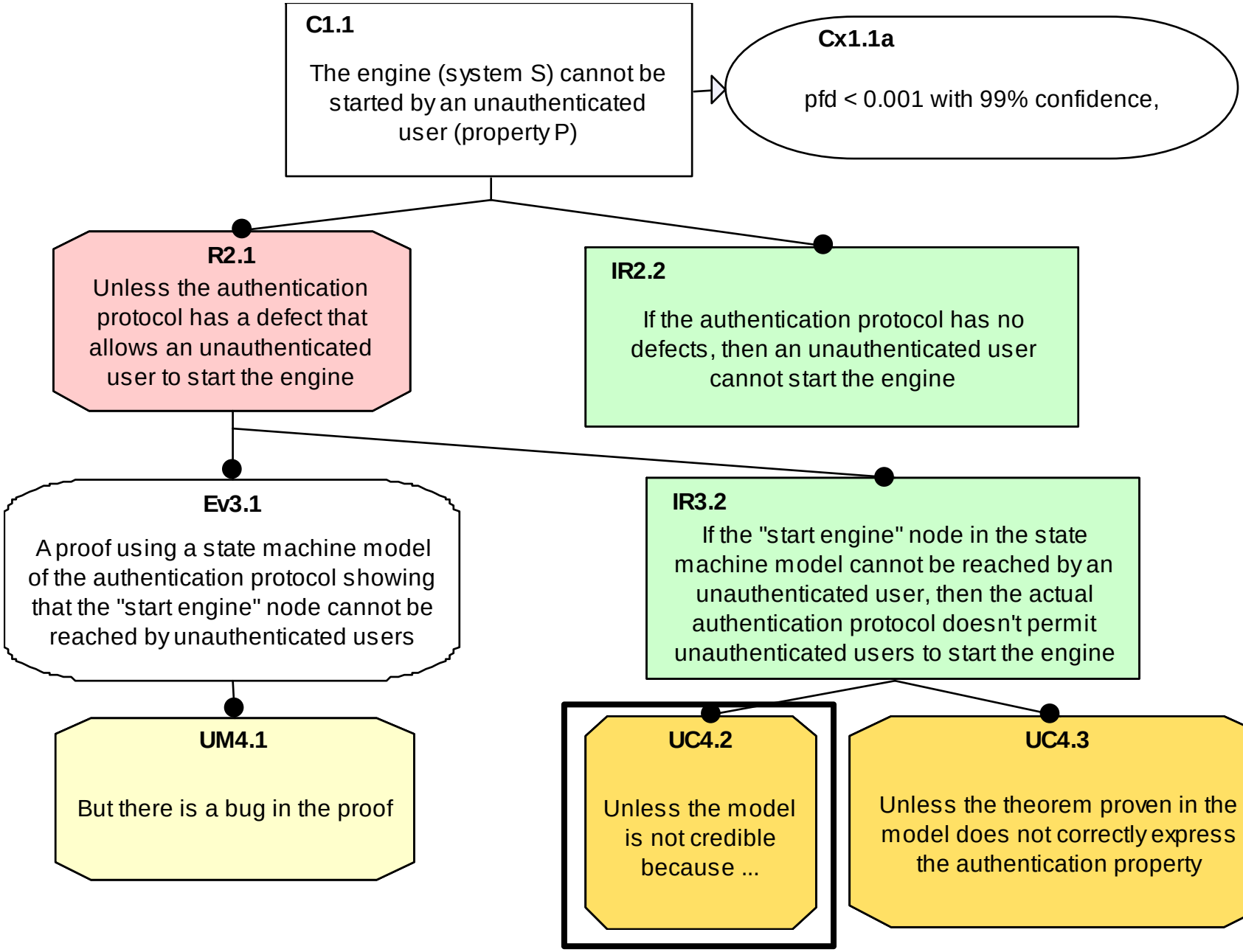
Calculating Confidence

Were fortunate to have a way of calculating how inaccuracies in the model would affect confidence in the conclusion

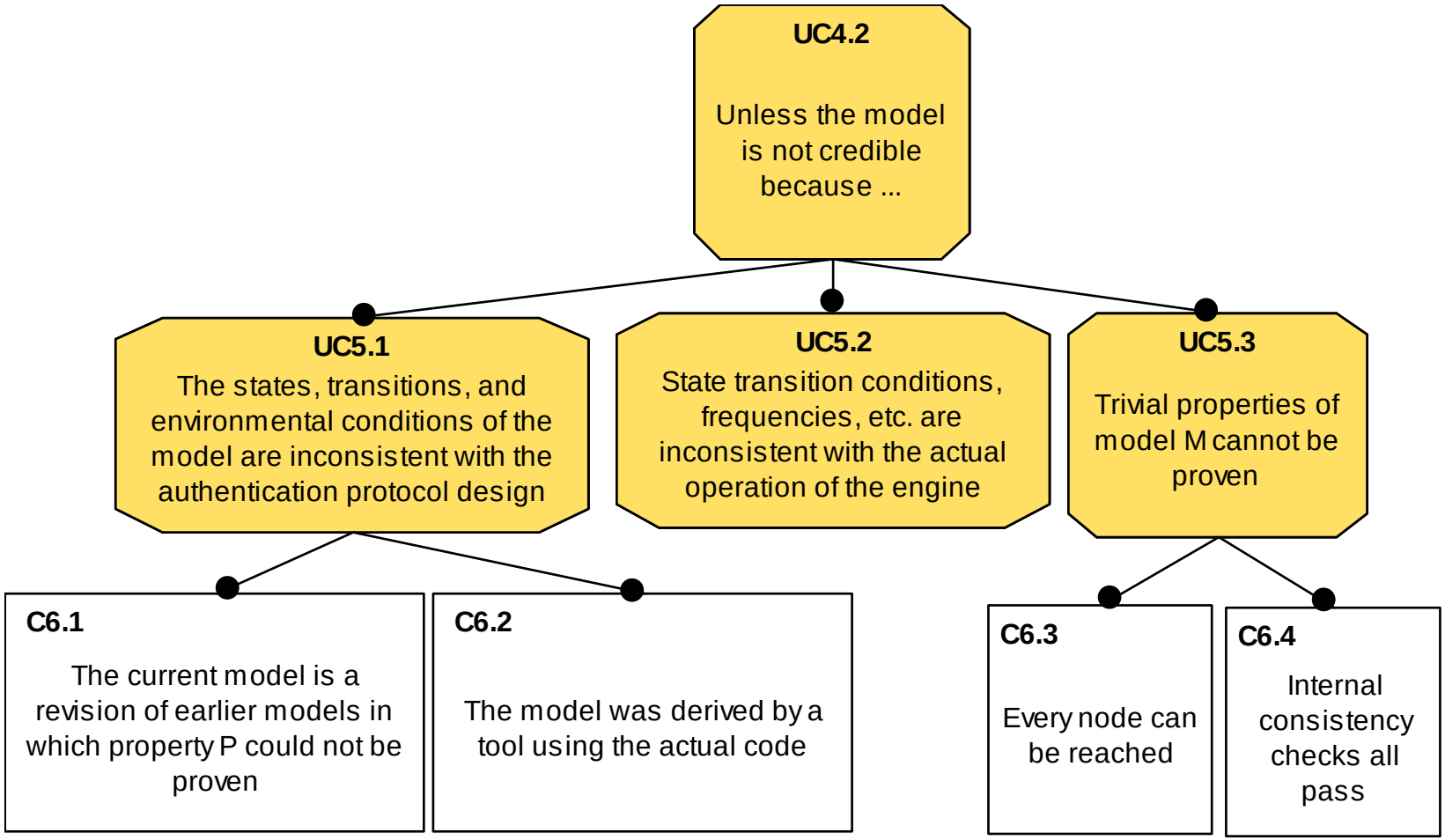
- Probabilistic variations in the model
- Affect confidence gained from the proof
- The analysis suggests where to strengthen the case

© 2015 Carnegie Mellon University


C1.1
The engine (system S) cannot be started by an unauthenticated user (property P)
Cx1.1a
pfd < 0.001 with 99% confidence,
R2.1
Unless the authentication protocol has a defect that allows an unauthenticated user to start the engine
IR2.2
If the authentication protocol has no defects, then an unauthenticated user cannot start the engine
Ev3.1
A proof using a state machine model of the authentication protocol showing that the "start engine" node cannot be reached by unauthenticated users
UM4.1
But there is a bug in the proof


C1.1
The engine (system S) cannot be started by an unauthenticated user (property P)
Cx1.1a
pfd < 0.001 with 99% confidence,
R2.1
Unless the authentication protocol has a defect that allows an unauthenticated user to start the engine
IR2.2
If the authentication protocol has no defects, then an unauthenticated user cannot start the engine
Ev3.1
A proof using a state machine model of the authentication protocol showing that the "start engine" node cannot be reached by unauthenticated users
IR3.2
If the "start engine" node in the state machine model cannot be reached by an unauthenticated user, then the actual authentication protocol doesn't permit unauthenticated users to start the engine
UM4.1
But there is a bug in the proof
UC4.2
Unless the model is not credible because ...
UC4.3
Unless the theorem proven in the model does not correctly express the authentication property

Model Credibility Evidence



© 2015 Carnegie Mellon University

Summary

Used Eliminative Argumentation to explore role of proofs in an AC

Considered how to use the proof as a guide for estimating the extent to which one can have confidence in the application of the proof result to the real world

- Modeling inaccuracies

© 2015 Carnegie Mellon University

Contact Information

John Goodenough
Telephone: +1 412.390.4043
Email: jbg@sei.cmu.edu

Chuck Weinstock
Telephone: +1 412.268.7719
Email: weinstock@sei.cmu.edu

© 2015 Carnegie Mellon University