5 criteria for **credibility**

Tenth Software Certification Consortium
Silver Spring, MD · January 7-8, 2013

Daniel Jackson
CSAIL, MIT

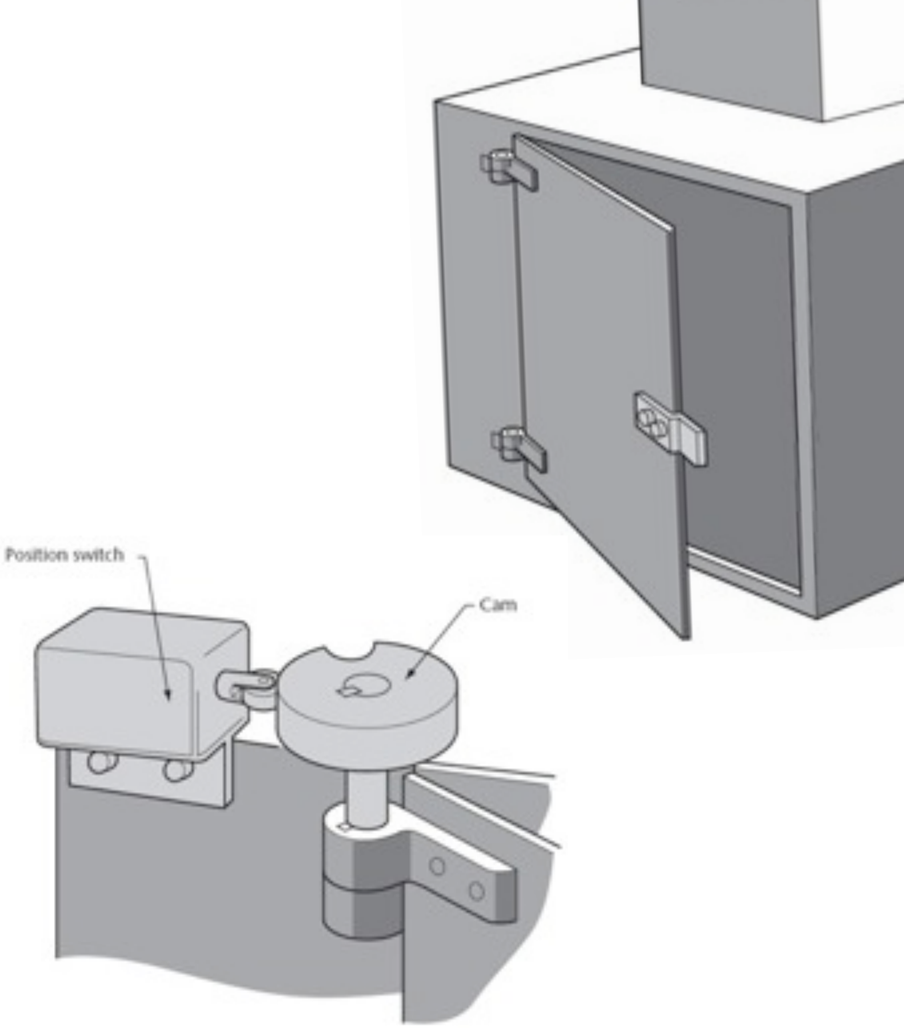
caveats

caveats

these criteria are

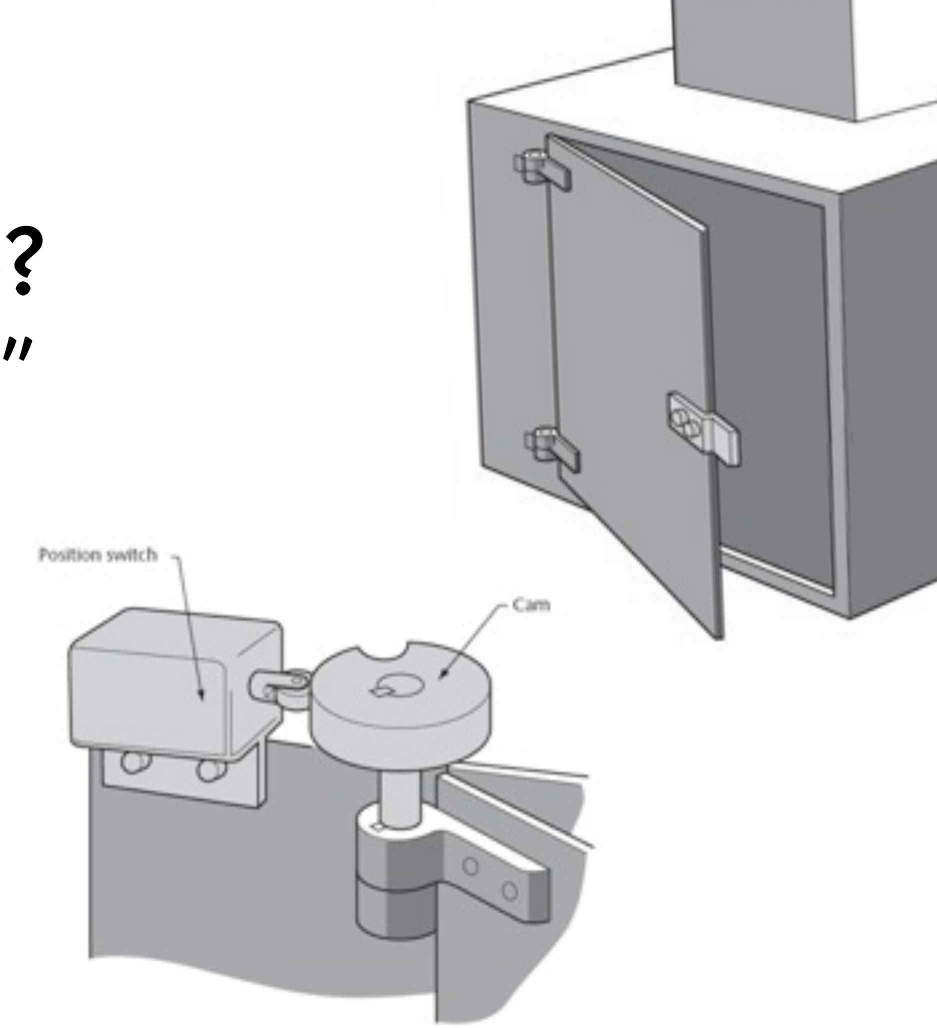
- not new
- not mine
- not enough

the case is self-contained


Position switch
Cam

does the case include process evidence?

- “C was tested with full branch coverage”
- “S was built using IEC61508”
- “requirements were reviewed by QA”

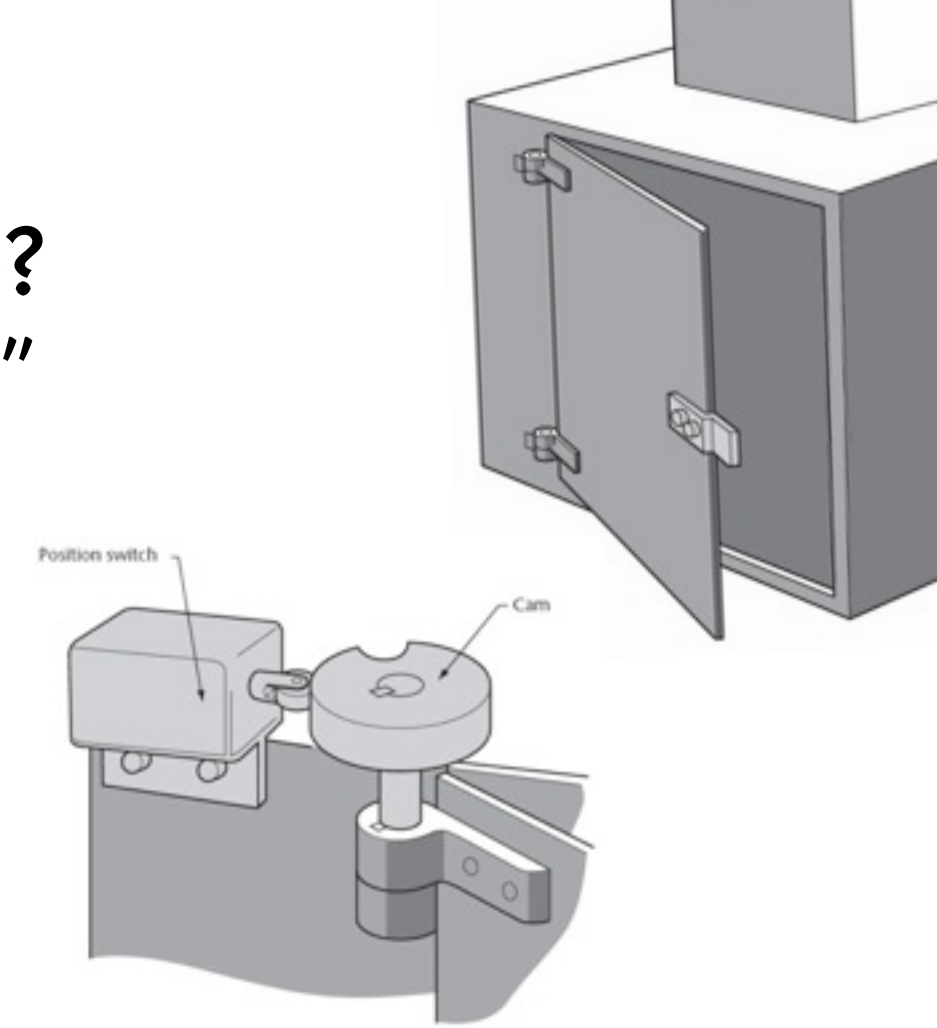


does the case include process evidence?

- "C was tested with full branch coverage"
- "S was built using IEC61508"
- "requirements were reviewed by QA"

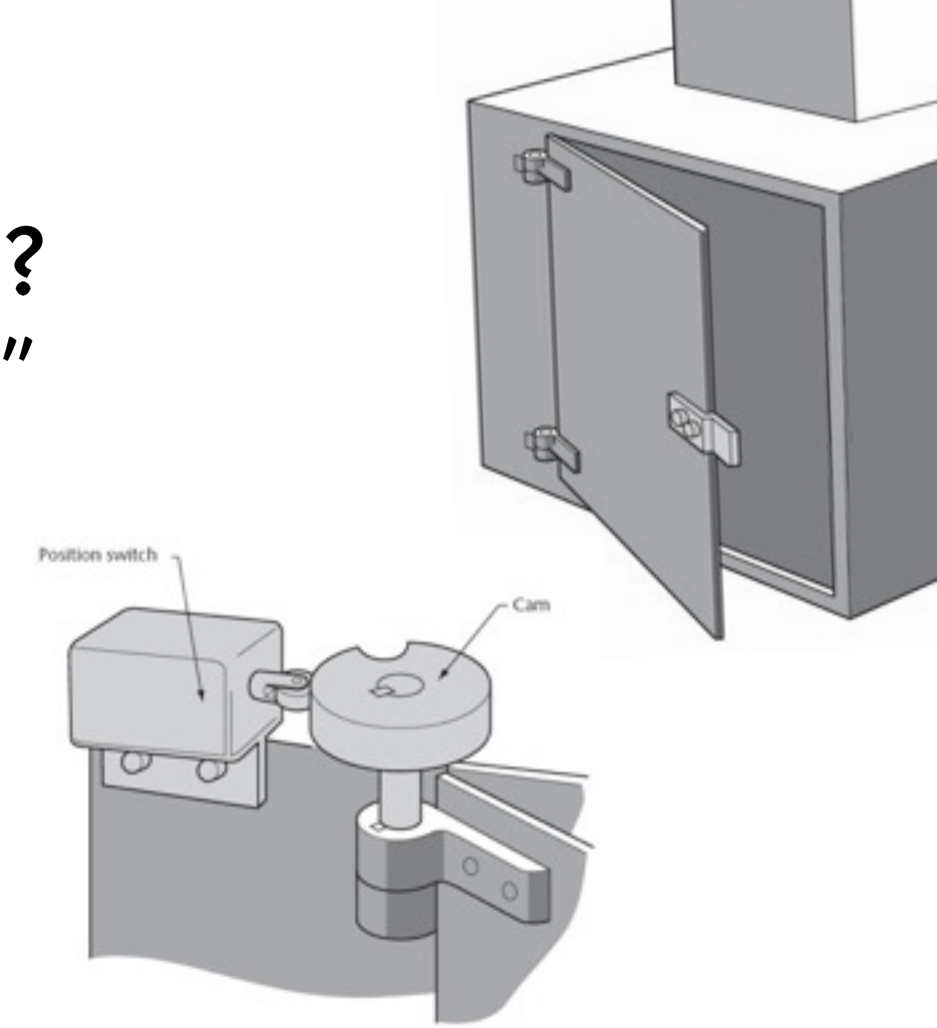
process arguments

- are arguments by "delegation"
- have minimal credibility
- OK for consumers, not for producers



does the case include process evidence?

- “C was tested with full branch coverage”
- “S was built using IEC61508”
- “requirements were reviewed by QA”



process arguments

- are arguments by “delegation”
- have minimal credibility
- OK for consumers, not for producers

consequences

- structure assurance case around product, not process

Saylor crash site
August 28, 2009

http://www.nap.edu/catalog.php?record_id=13342

Saylor crash site
August 28, 2009

[NASA's Engineering and Safety Center (NESC)] investigators used multiple tools to analyze software logic paths and to examine the programming code for paths that might lead to unintended acceleration. These extensive testing and analytic efforts did not uncover any evidence of problems, but the team pointed out that **no practical amount of testing and analysis can guarantee that software is free of faults**. The NESC software analysts reported that **certain characteristics of the subject software (from a 2005 Camry) hindered the testing**. For example, they found that the code structure relied on the use of a single large memory space... **This lack of modularity reportedly precluded automated analysis** and required more time-consuming manual inspection by analysts. Thus, the NESC team's technical description of its analysis suggested a concern that **the software was not structured to facilitate assessments of dependability to a high degree of confidence.**

—The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration

http://www.nap.edu/catalog.php?record_id=13342 the case is complete

requirements

- are in the world, not at the interface
- about humans, physical things
- rarely about computers

requirements

- are in the world, not at the interface
- about humans, physical things
- rarely about computers

view system as a chain

- each link in the chain is a component
- or user, operator, peripheral…

requirements

- are in the world, not at the interface
- about humans, physical things
- rarely about computers

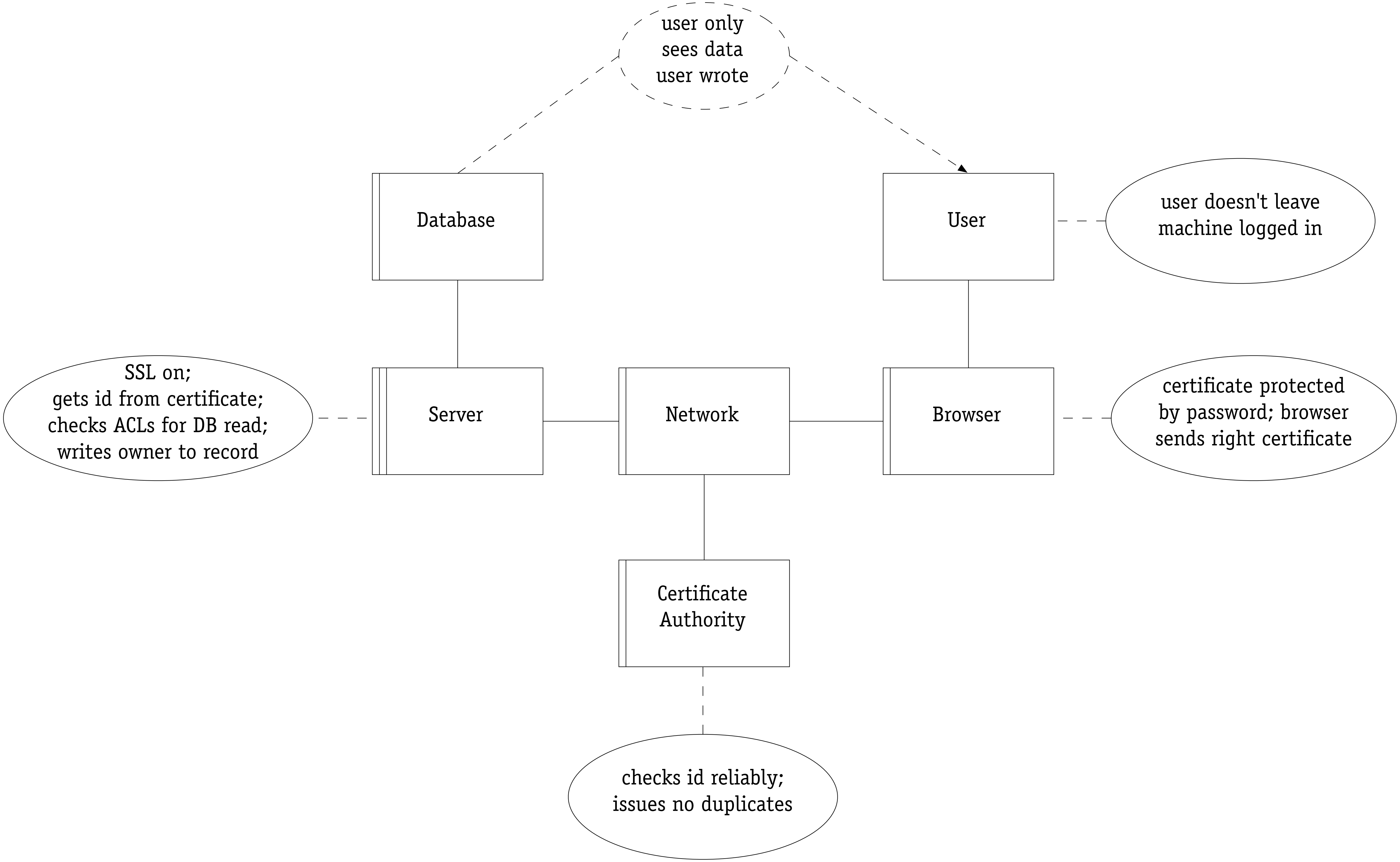
view system as a chain

- each link in the chain is a component
- or user, operator, peripheral…

consequences

- start with context diagram
- express requirements end-to-end
- validate domain assumptions

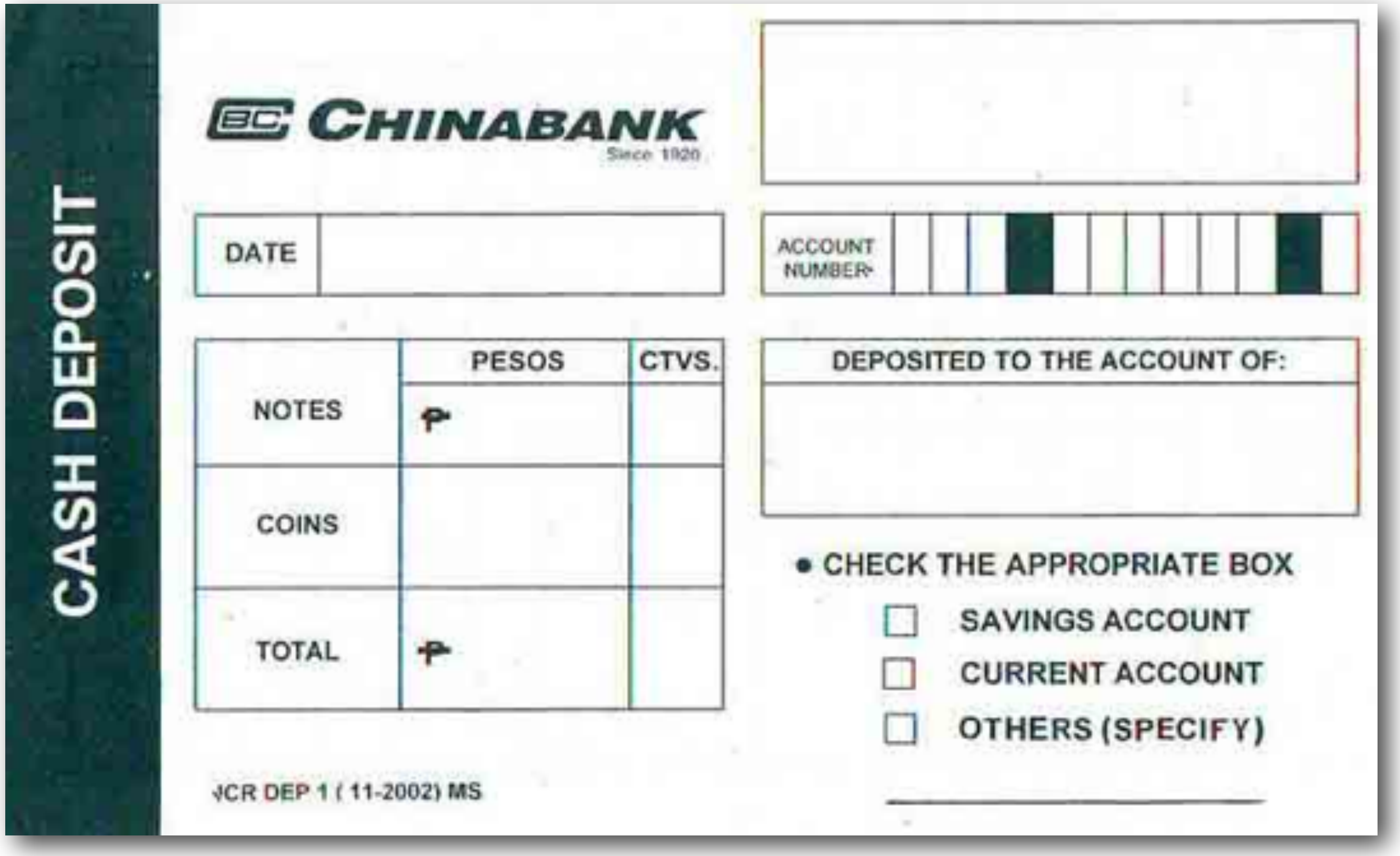
web security



user only sees data user wrote
Database
User
user doesn't leave machine logged in
SSL on;
gets id from certificate;
checks ACLs for DB read;
writes owner to record
Server
Network
Browser
certificate protected by password; browser sends right certificate
Certificate Authority
checks id reliably;
issues no duplicates

frank abagnale's deposit fraud

frank abagnale's deposit fraud



CASH DEPOSIT

CHINABANK
Since 1920

DATE

ACCOUNT NUMBER

	PESOS	CTVS.
NOTES	₱	
COINS		
TOTAL	₱	

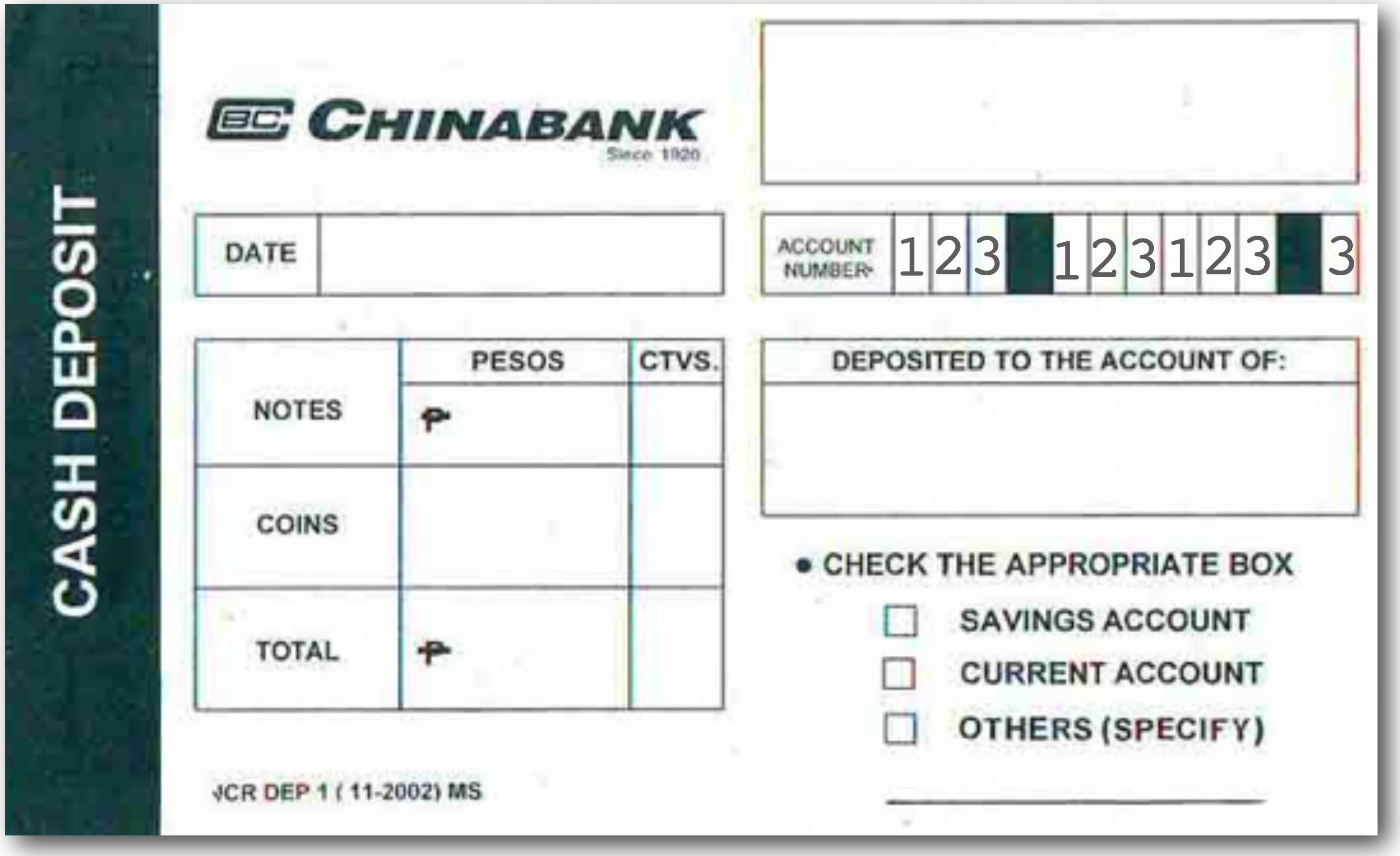
DEPOSITED TO THE ACCOUNT OF:

● CHECK THE APPROPRIATE BOX

□ SAVINGS ACCOUNT
□ CURRENT ACCOUNT
□ OTHERS (SPECIFY)

NCR DEP 1 (11-2002) MS

frank abagnale's deposit fraud



CASH DEPOSIT

CHINABANK
Since 1920

DATE

ACCOUNT NUMBER 1 2 3 ■ 1 2 3 1 2 3 ■ 3

	PESOS	CTVS.
NOTES	₱	
COINS		
TOTAL	₱	

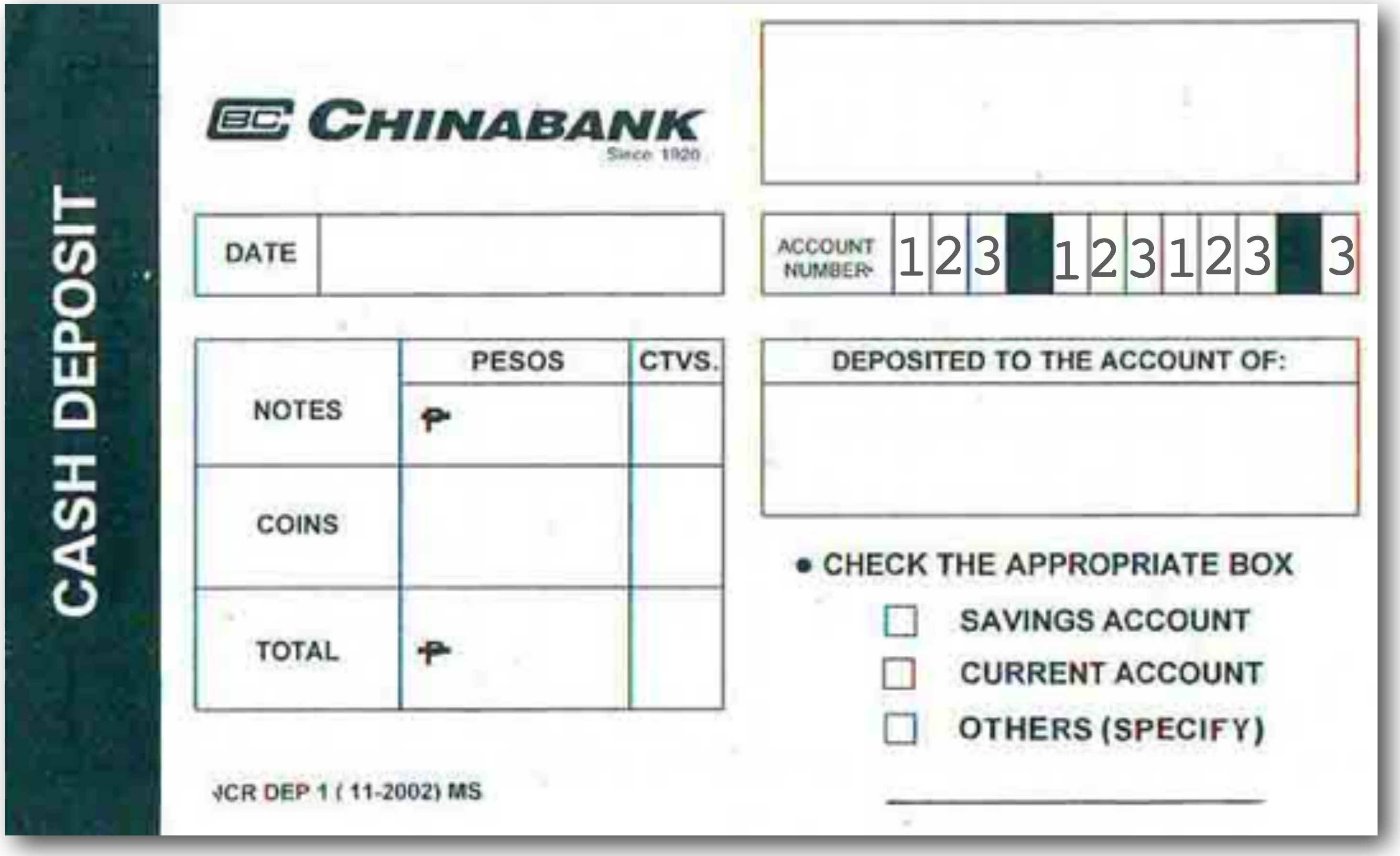
DEPOSITED TO THE ACCOUNT OF:

● CHECK THE APPROPRIATE BOX

□ SAVINGS ACCOUNT
□ CURRENT ACCOUNT
□ OTHERS (SPECIFY)

NCR DEP 1 (11-2002) MS

frank abagnale's deposit fraud



CASH DEPOSIT

CHINABANK
Since 1920

DATE

ACCOUNT NUMBER 1 2 3 ■ 1 2 3 1 2 3 ■ 3

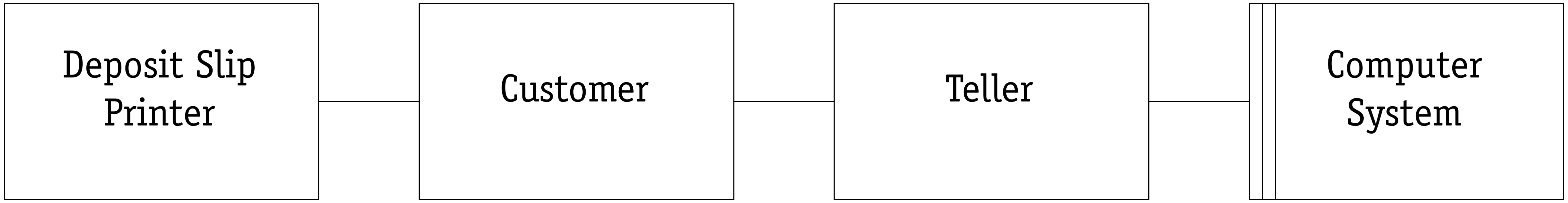
	PESOS	CTVS.
NOTES	₱	
COINS		
TOTAL	₱	

DEPOSITED TO THE ACCOUNT OF:

- CHECK THE APPROPRIATE BOX

□ SAVINGS ACCOUNT
□ CURRENT ACCOUNT
□ OTHERS (SPECIFY)

NCR DEP 1 (11-2002) MS



Deposit Slip Printer

Customer

Teller

Computer System

the case is logical

argument must be logically consistent

argument must be logically consistent

even in a small argument

- easy to make mistakes
- effect of “wishful thinking”

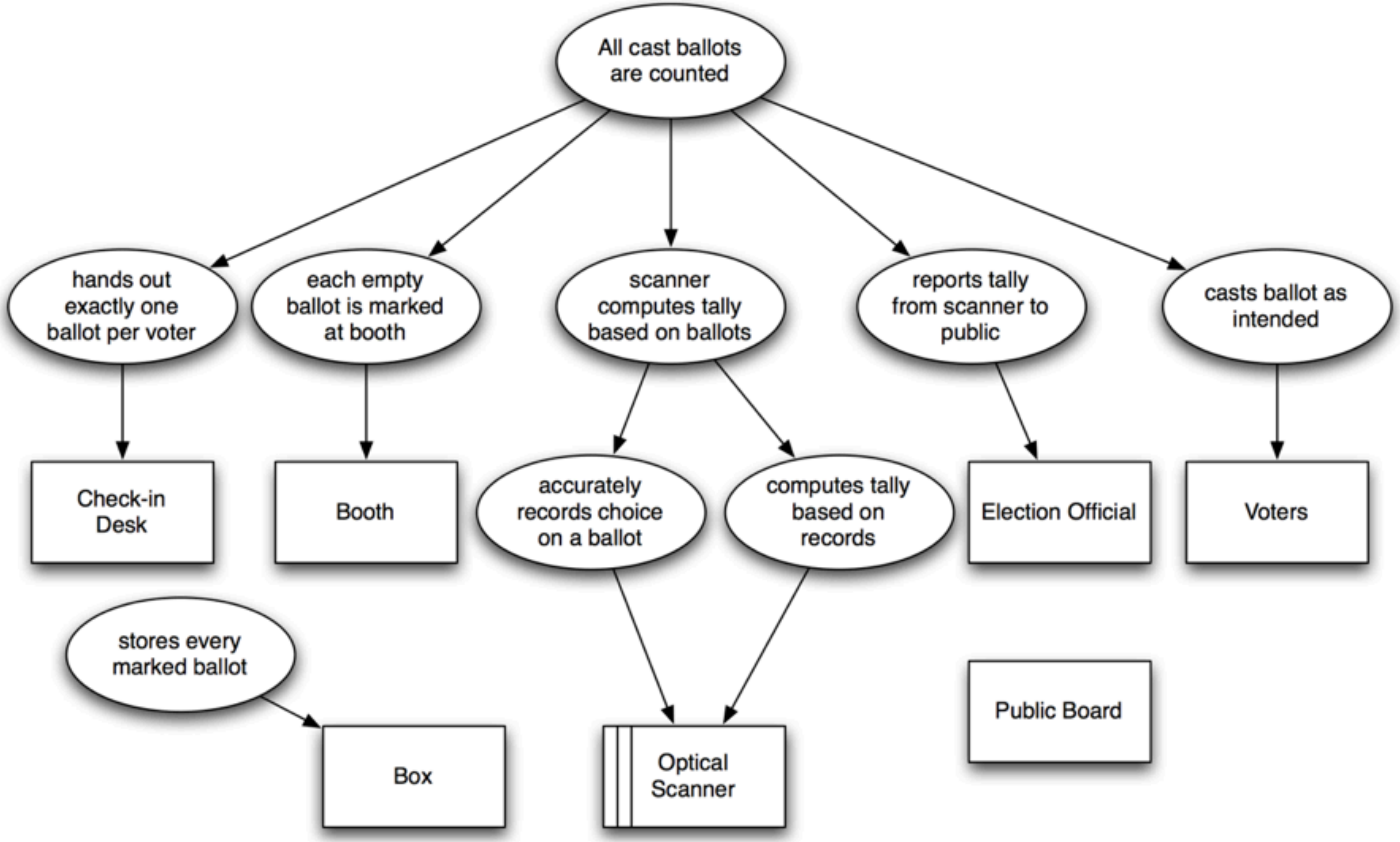
argument must be logically consistent

even in a small argument

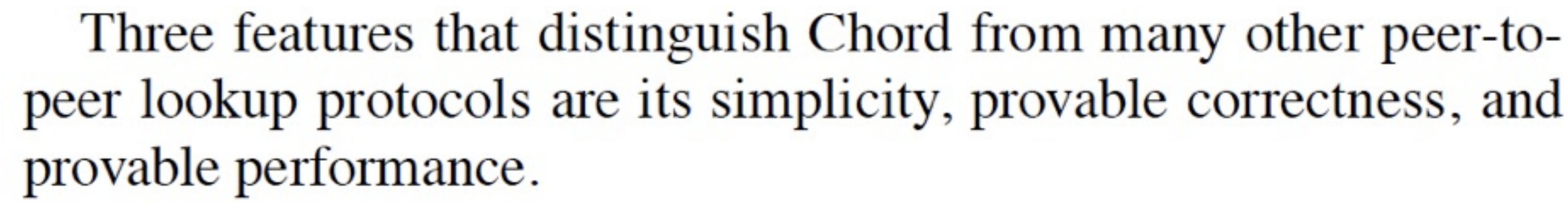
- easy to make mistakes
- effect of “wishful thinking”

consequences

- must use tools
- not just for subarguments
- for composing them too!


All cast ballots are counted
hands out exactly one ballot per voter
each empty ballot is marked at booth
scanner computes tally based on ballots
reports tally from scanner to public
casts ballot as intended
Check-in Desk
Booth
accurately records choice on a ballot
computes tally based on records
Election Official
Voters
stores every marked ballot
Box
Optical Scanner
Public Board

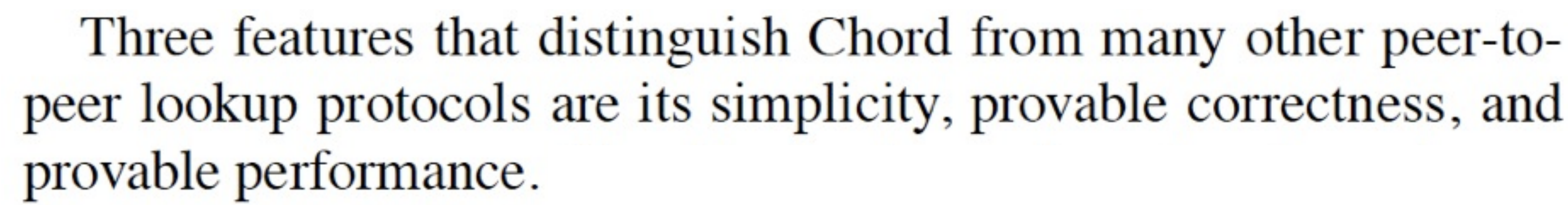
chord: a “provably correct” protocol



Three features that distinguish Chord from many other peer-to-peer lookup protocols are its simplicity, provable correctness, and provable performance.

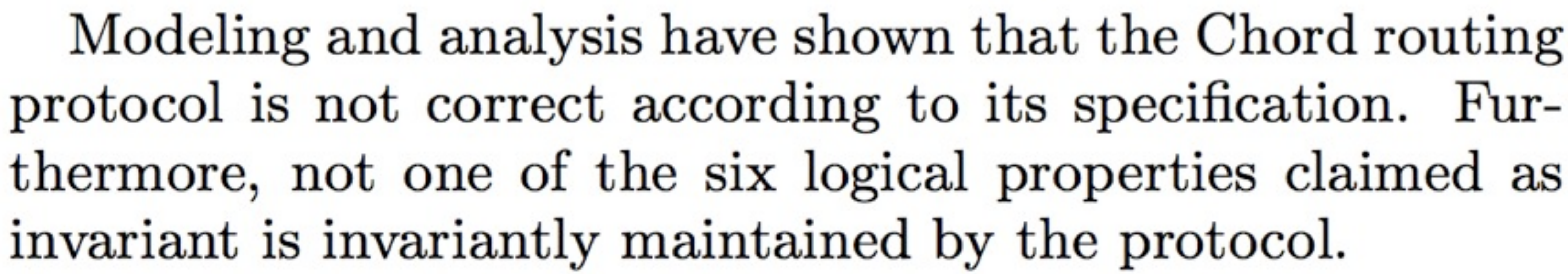
Ion Stoica et al. Chord: A Scalable Peer to Peer Lookup Service for Internet Applications, SIGCOMM 2001 (also TON, 2003)

chord: a “provably correct” protocol



Three features that distinguish Chord from many other peer-to-peer lookup protocols are its simplicity, provable correctness, and provable performance.

Ion Stoica et al. Chord: A Scalable Peer to Peer Lookup Service for Internet Applications, SIGCOMM 2001 (also TON, 2003)



Modeling and analysis have shown that the Chord routing protocol is not correct according to its specification. Furthermore, not one of the six logical properties claimed as invariant is invariantly maintained by the protocol.

Pamela Zave. Invariant-Based Verification of Routing Protocols: The Case of Chord, 2009 the case is sound

onGround $\overset{?}{\Leftrightarrow}$ wheelRotating

argument can be logical but unsound

- just doesn’t match reality!

$$\text{onGround} \overset{?}{\Leftrightarrow} \text{wheelRotating}$$

argument can be logical but unsound

- just doesn’t match reality!

problems with phenomena

- bad surrogates (eg Warsaw Airbus)
- abstract (power attack on smartcard)
- most often: not clear

onGround $\overset{?}{\Leftrightarrow}$ wheelRotating

argument can be logical but unsound

- just doesn’t match reality!

problems with phenomena

- bad surrogates (eg Warsaw Airbus)
- abstract (power attack on smartcard)
- most often: not clear

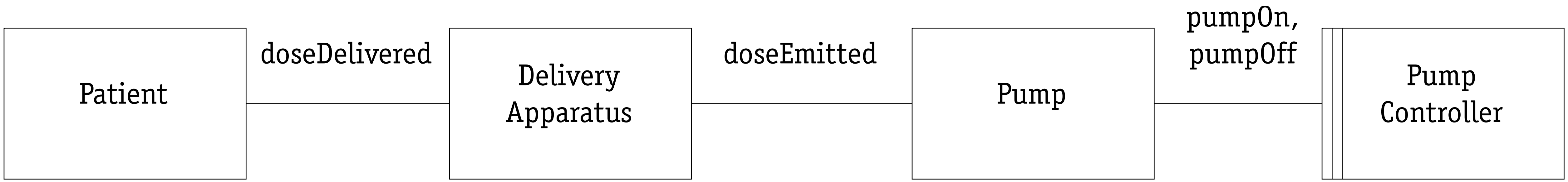
onGround $\overset{?}{\Leftrightarrow}$ wheelRotating

consequences

- as first step in requirements, list phenomena & document interfaces between domains

example: epidural pump

doseEmitted $\overset{?}{\Leftrightarrow}$ doseDelivered



Patient

doseDelivered

Delivery Apparatus

doseEmitted

Pump

pumpOn, pumpOff

Pump Controller

the case is simple

complexity undermines credibility

- rely on as little as possible: few parts, small properties
- dangerous if no single person understands whole case
- automated analyses (esp. model checking) are brittle

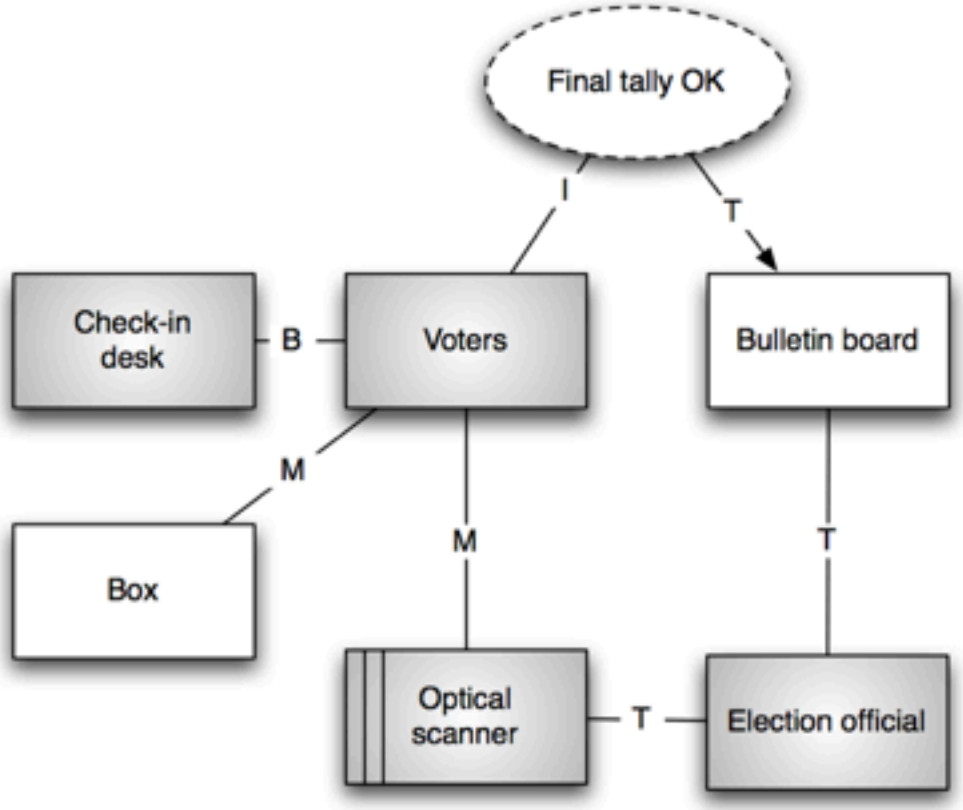
complexity undermines credibility

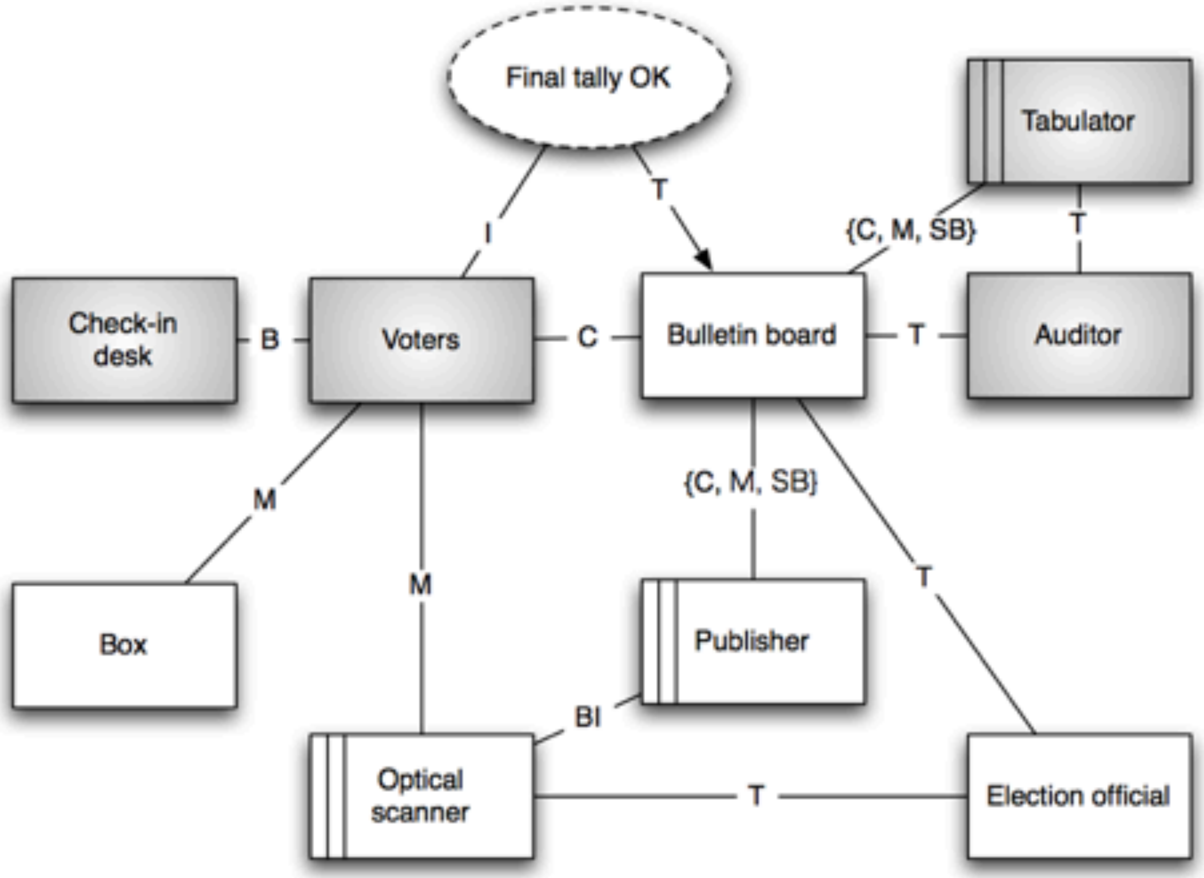
- rely on as little as possible: few parts, small properties
- dangerous if no single person understands whole case
- automated analyses (esp. model checking) are brittle

consequences

- give up on complete requirements: prioritize!
- identify trusted bases, per property
- case determines design, not vice versa

example: voting design





references

references

product not process

› *Software for Dependable Systems: Sufficient Evidence?* National Academies, 2007.

references

product not process

- *Software for Dependable Systems: Sufficient Evidence?* National Academies, 2007.

end to end requirements

- David Parnas & Jan Madey. Functional Documents for Computer Systems. *SCP*, 25 (1995)
- Carl Gunter, Elsa Gunter, Michael Jackson & Pamela Zave. A Reference Model for Requirements and Specifications. *IEEE Software*, May/June 2000.

references

product not process

- *Software for Dependable Systems: Sufficient Evidence?* National Academies, 2007.

end to end requirements

- David Parnas & Jan Madey. Functional Documents for Computer Systems. *SCP*, 25 (1995)
- Carl Gunter, Elsa Gunter, Michael Jackson & Pamela Zave. A Reference Model for Requirements and Specifications. *IEEE Software*, May/June 2000.

phenomena

- Michael Jackson. *Problem Frames*. Addison Wesley, 2001.

references

product not process

- *Software for Dependable Systems: Sufficient Evidence?* National Academies, 2007.

end to end requirements

- David Parnas & Jan Madey. Functional Documents for Computer Systems. *SCP*, 25 (1995)
- Carl Gunter, Elsa Gunter, Michael Jackson & Pamela Zave. A Reference Model for Requirements and Specifications. *IEEE Software*, May/June 2000.

phenomena

- Michael Jackson. *Problem Frames*. Addison Wesley, 2001.

logical analysis with tools

- Eunsuk Kang. *A Framework for Dependability Analysis of Software Systems with Trusted Bases*. SM Thesis, 2010, MIT.

references

product not process

- *Software for Dependable Systems: Sufficient Evidence?* National Academies, 2007.

end to end requirements

- David Parnas & Jan Madey. Functional Documents for Computer Systems. *SCP*, 25 (1995)
- Carl Gunter, Elsa Gunter, Michael Jackson & Pamela Zave. A Reference Model for Requirements and Specifications. *IEEE Software*, May/June 2000.

phenomena

- Michael Jackson. *Problem Frames*. Addison Wesley, 2001.

logical analysis with tools

- Eunsuk Kang. *A Framework for Dependability Analysis of Software Systems with Trusted Bases*. SM Thesis, 2010, MIT.

trusted bases

- Jerry Saltzer, David Reed & David Clark. End-to-end arguments in system design. *TOCS*, 2.4 (1984).
- Eunsuk Kang & Daniel Jackson. Dependability Arguments with Trusted Bases. RE 2010.