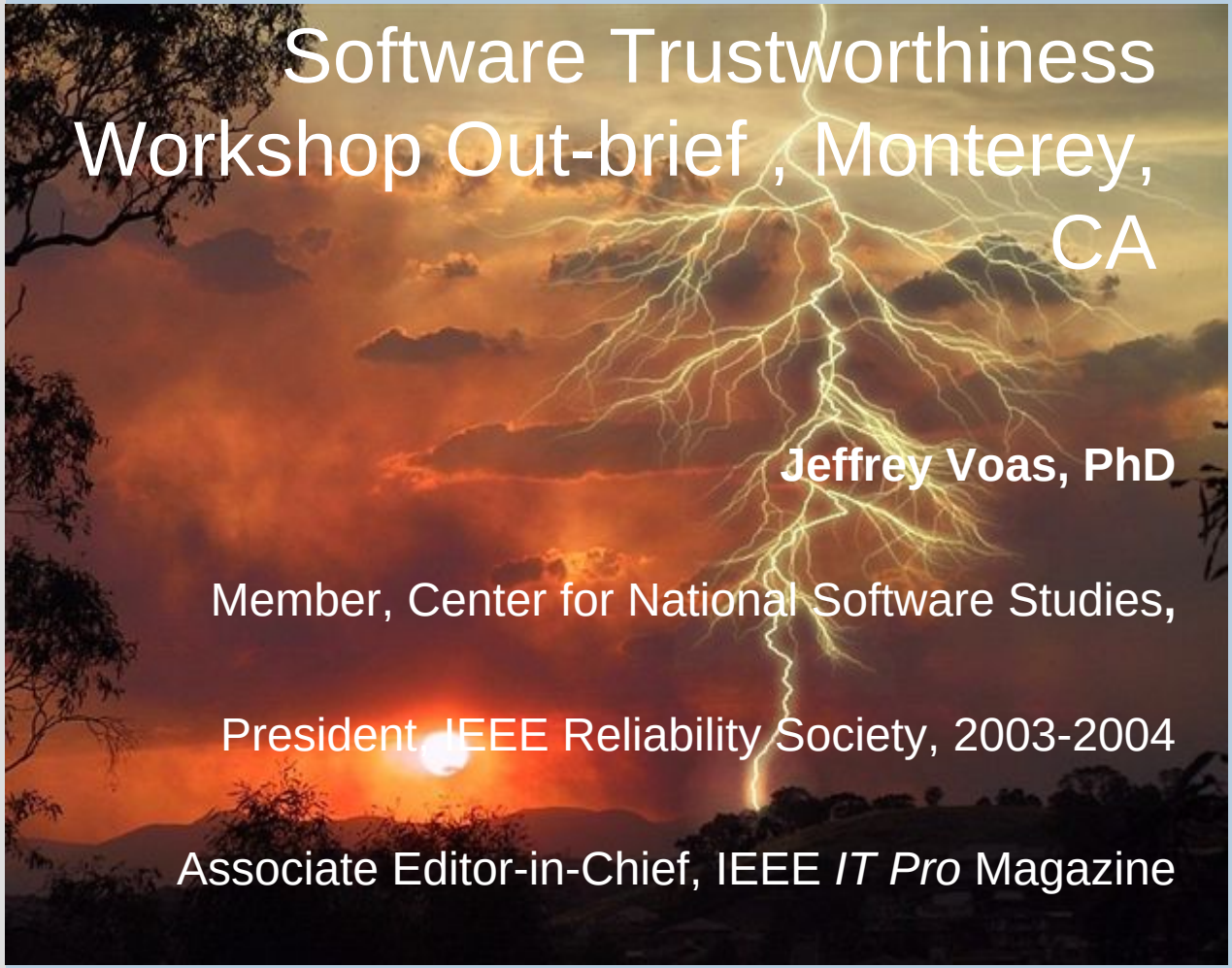
cigital

Software Trustworthiness Workshop Out-brief , Monterey, CA



Jeffrey Voas, PhD

Member, Center for National Software Studies,

President, IEEE Reliability Society, 2003-2004

Associate Editor-in-Chief, IEEE *IT Pro* Magazine

IEEE

ReliabilitySociety

cigital

Monterey, CA April 8-9, 2004

- Three Co-Chairs: Dr. Bret Michael (Naval Postgraduate School), Mr. Rick Linger (SEI), Dr. Jeffrey Voas (Cigital Inc.)
- Approximately 28 attendees
- Naval Postgraduate School, Monterey, CA
- 1.5 days
- Breakout groups: Legal, Technology, Market

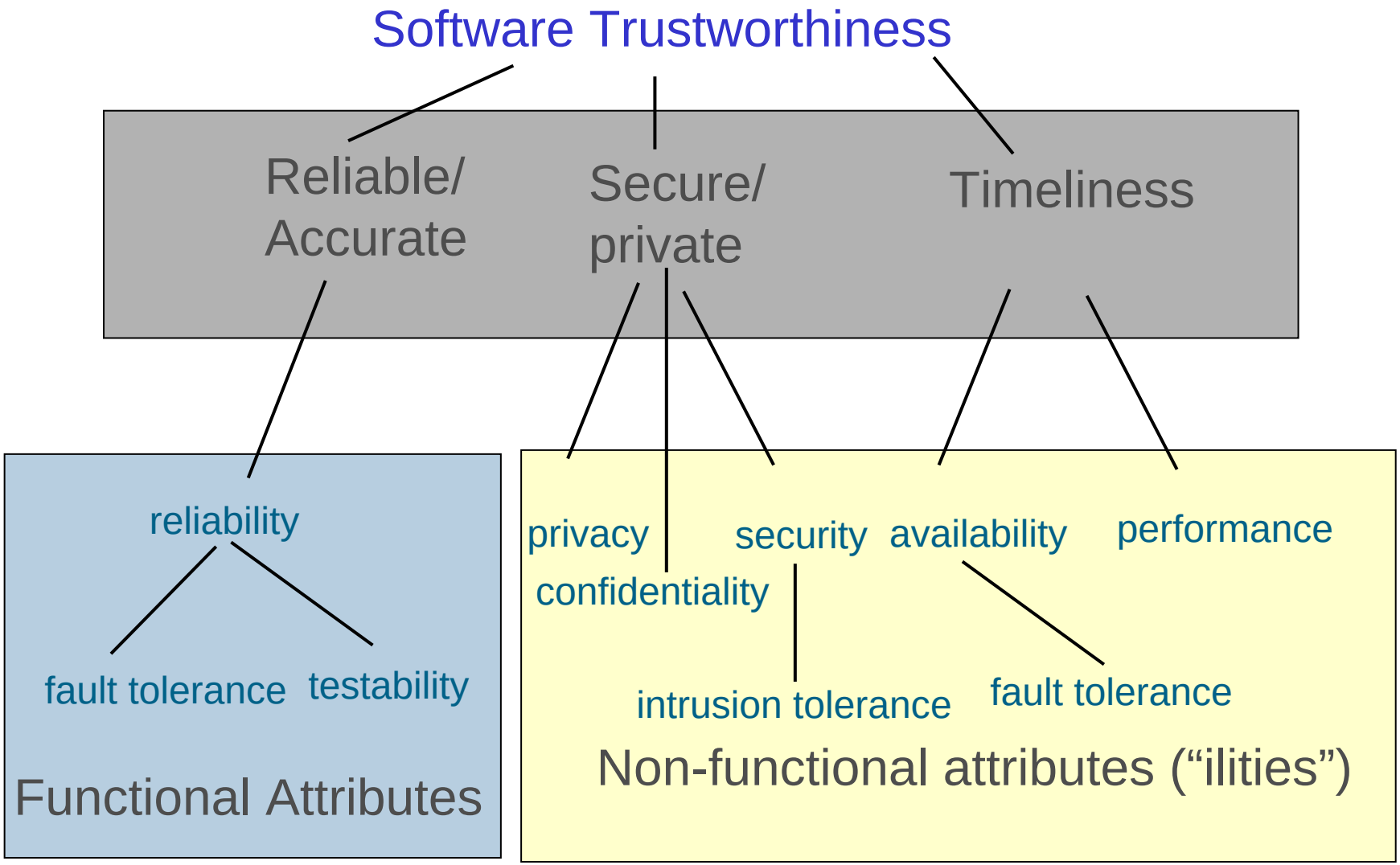
cigital

Four Key Questions

- (1) How should “software trustworthiness” be defined and measured?
- (2) Is the degree to which software products are being shipped with known latent defects acceptable?
- (3) What is the state-of-the-art of software engineering with respect to software trustworthiness, and what is the state of practice in industry?
- (4) Is there a need for an Independent software testing and certification organization, similar to an Underwriter’s Laboratory, to perform assessments of trustworthiness?

Question #1

Defining Software Trustworthiness


Software Trustworthiness
Reliable/
Accurate
Secure/
private
Timeliness
reliability
fault tolerance
testability
Functional Attributes
privacy
confidentiality
security
availability
performance
intrusion tolerance
fault tolerance
Non-functional attributes (“ilities”)

cigital

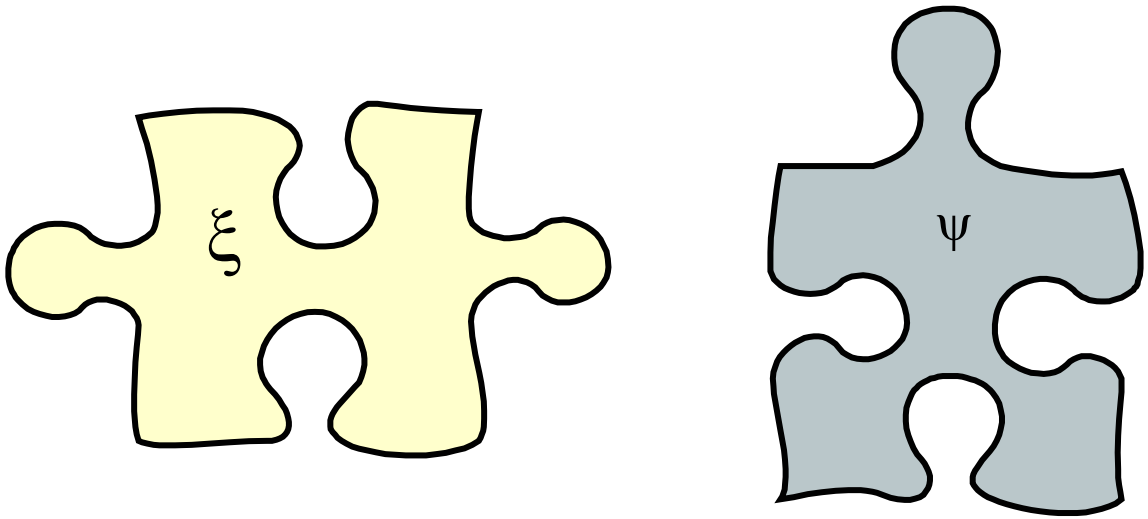
Statement

Software's Trustworthiness is some combination of:

(1) the degree to which the *functional* requirements are met, as well as, (2) the degree to which the *non-functional* requirements are met.

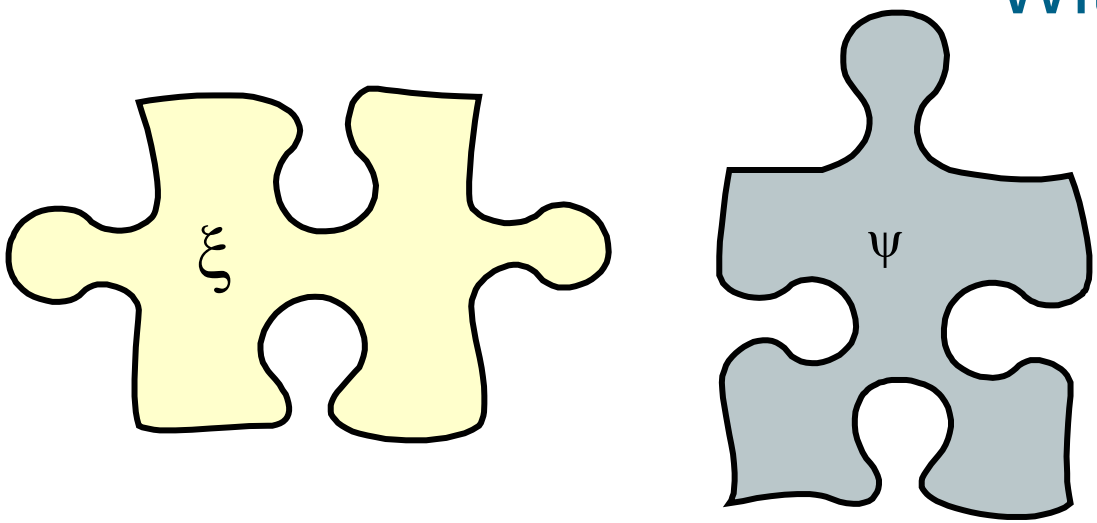
cigital

Two Components



cigital

With Attributes



ξ has the following properties:

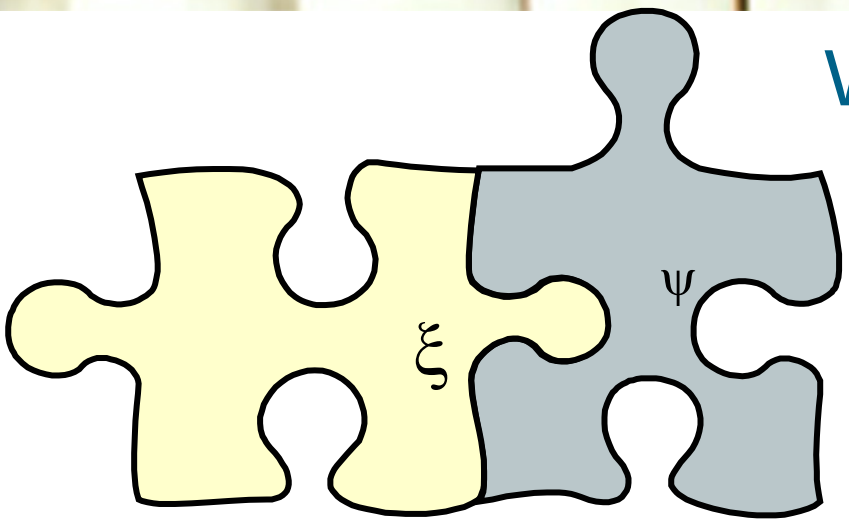
(*a*R, *b*P, *c*F, *d*Sa, *e*Se, *f*A, *g*T, *h*M)

ψ has the following properties:

(*i*R, *j*P, *k*F, *l*Sa, *m*Se, *n*A, *o*T, *p*M)

cigital

What Have You Got?



Then $F(\xi \circ \psi)$ will inherit some level of trustworthiness from the individual components. Is that level of quality an integer? Probability? An n-tuple of values? Color coded (green red yellow)?

Key Point: The composite trustworthiness must represent something from which predictions of future behavior can be made.

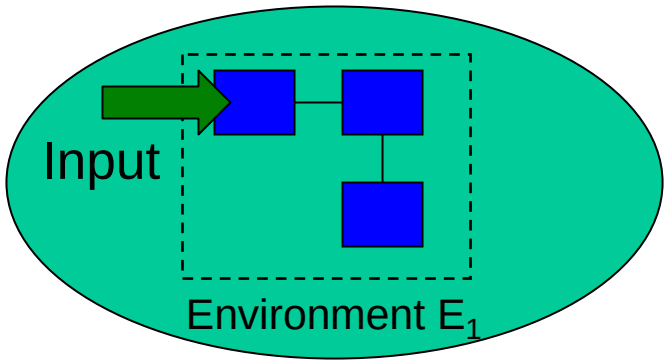
cigital

Difficult Because …

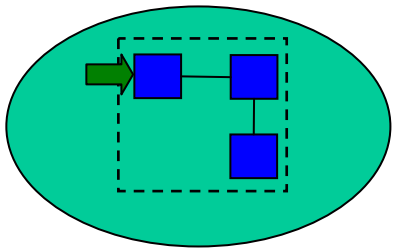
Trustworthiness attributes have little meaning in terms of their ability to be measured and traded off until they are defined in the context of the target system, i.e., their environment.

cigital

- ✓ Reliability
- Performance
- ✓ Fault Tolerance
- Safety
- Security
- ✓ Availability
- ✓ Testability
- Maintainability

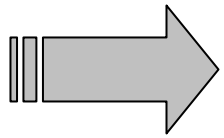


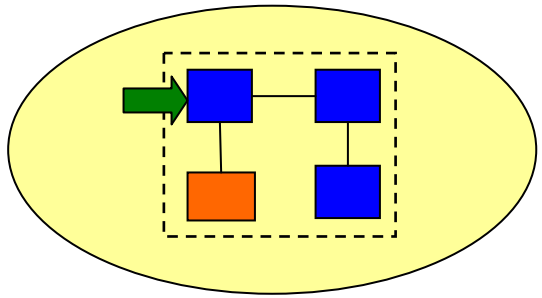
Trust ✓



Environment E_1

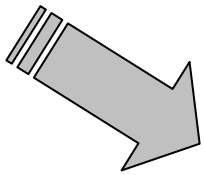
QoS

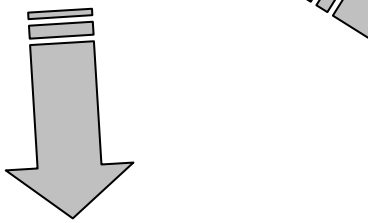


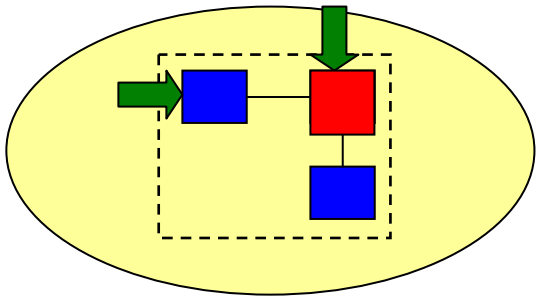


Trust ?

Environment E'_1

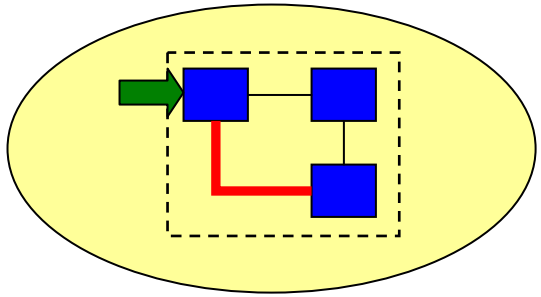






Trust ?

Environment E'_3



Trust ?

Environment E'_2

Question #2

Amount of Latent Defects Acceptable?

cigital

The Obvious Conclusion….

No , but at what cost to decrease the number of “*important*” defects?

cigital

Question #3

What is the state-of-the-art of software engineering with respect to software trustworthiness, and what is the state-of-the-practice in industry?

cigital

Universal Consensus

- The state-of-the-art of always beyond the state-of-the-practice.
- The state-of-the-practice needs justification to move further towards the state-of-the-art. This requires both the “total cost of ownership ROI” and an economic incentive.
- Regulation and standards can expedite this, but in a “push” mode versus “pull” mode.

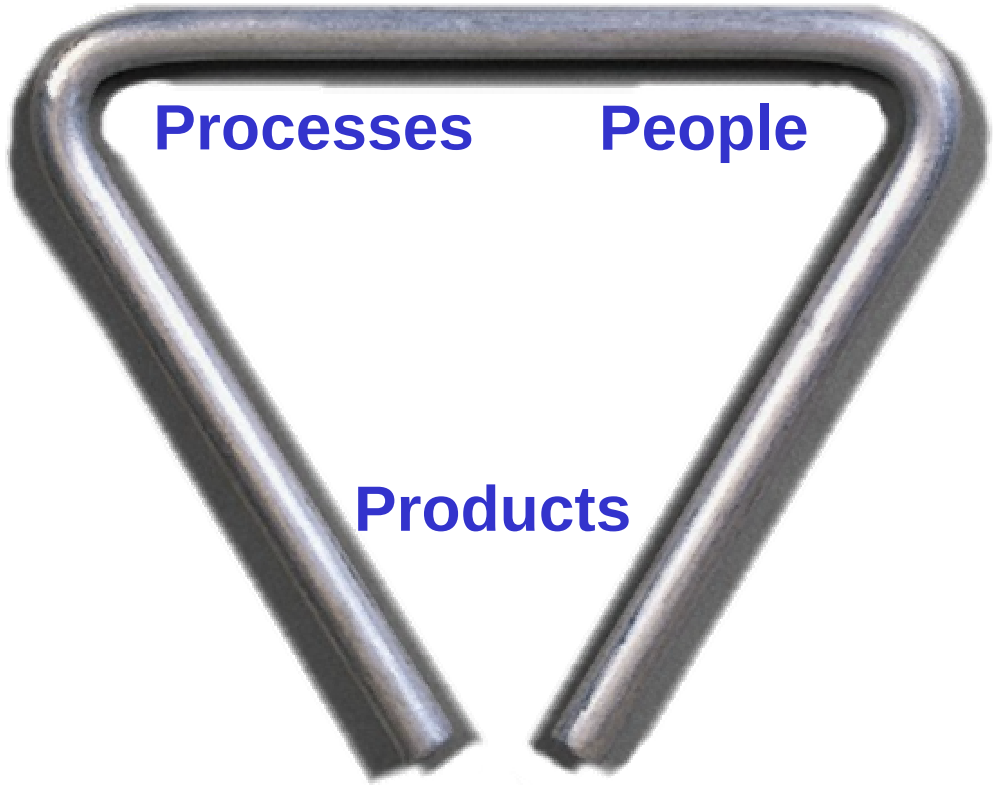
Question #4

Software certification via an organization like UL?

cigital

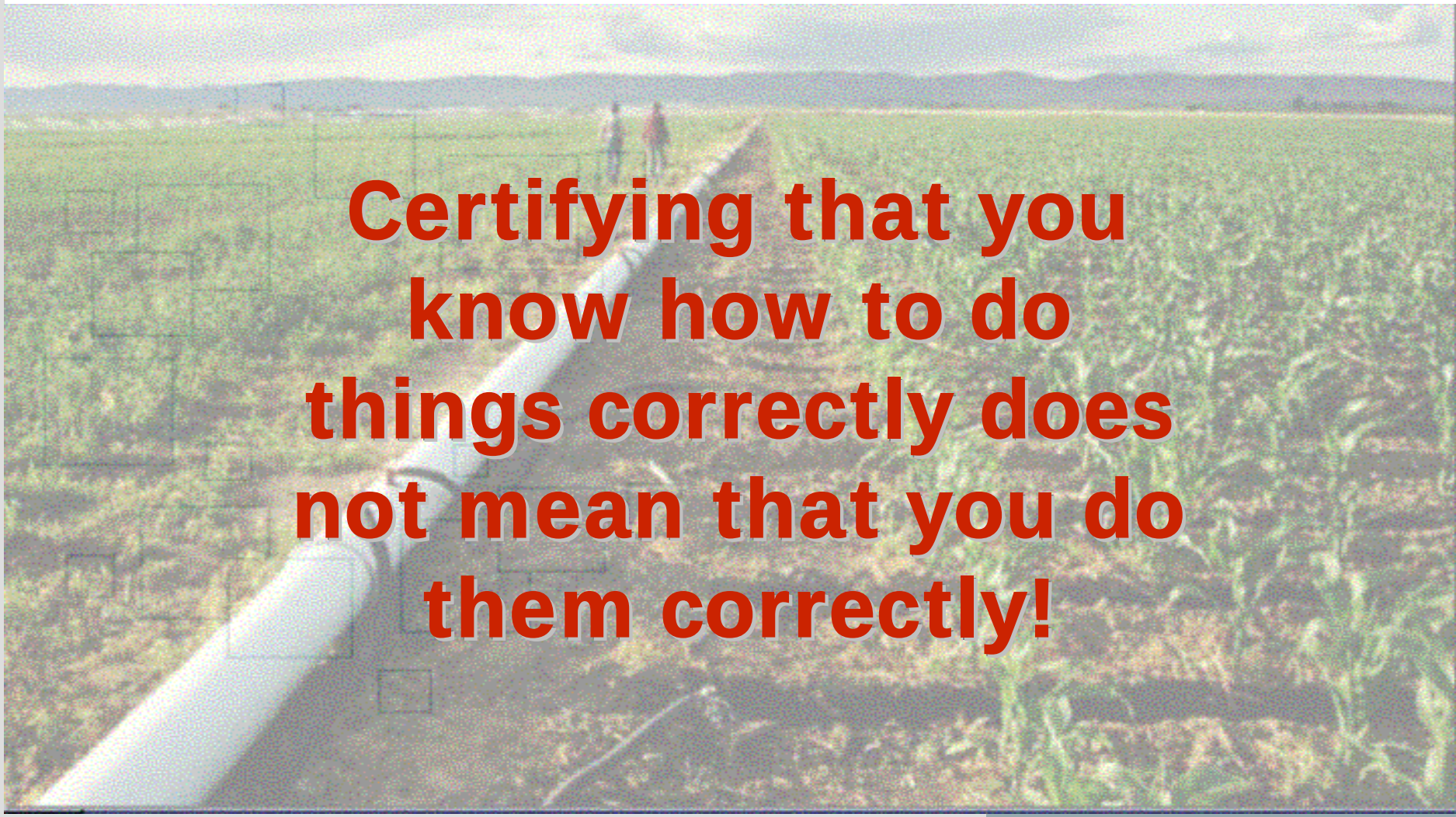
Three Schools of Thought

All cert. standards incorporate one or more of these perspectives



cigital

1. Process: Clean Pipes, Dirty Water?



2. People

The IEEE Computer Society has developed a program to certify software engineering professionals. This program provides formal recognition of professionals who have successfully achieved a level of proficiency commonly accepted and valued by the industry.

cigital

Serious Question

What does process maturity and personnel accreditation say specifically about how the software will behave in the future?

cigital

3. Product: The Software Itself

Spectrum of possibilities as to what a certificate proclaiming that some “quantified” level of quality has been built in could state --- it could say anything in the range between “Nothing” (*e.g.*, “here is a piece of software”, etc.) to “This software will always work perfectly under all conditions” (i.e., a 100% guarantee of perfection).

And So How Should Certification Criteria Be Created?

cigital

What Attribute is Being Certified?

- Reliability?
  - RTCA's DO178B (FAA)
- That the degree of testing done was appropriate?
  - RTCA's DO178B (FAA)
- Safety?
  - System (process) vs. component (product) safety
    - IEC 61508 vs. UL 1998
- Security?, Availability?, Fault Tolerance? Performance?, etc.
- That certain development procedures were followed?
  - SEI Capability Maturity Model
  - ISO 900x

cigital

Key Challenges from Monterey Meeting

- ***Improving our willingness to build software trustworthiness into systems and products from their conceptualization***
- ***Bettering our ability to both identify and characterize the attributes of a system that contribute or detract from software trustworthiness***
- ***Providing stakeholders with both "practical" and "justifiable" levels of software trustworthiness***
- ***Developing a means for assessing the trustworthiness of both families of products and systems-of-systems***
- ***Producing empirical evidence to determine how specific software engineering processes, practices, and methods lead to the realization of trustworthy software***
- ***Perfecting our ability to communicate with stakeholders about the topic of software trustworthiness***

cigital

Key Challenges from Monterey Meeting (continued)

- ***Investigating the feasibility of creating independent organizations to evaluate software trustworthiness***
- ***Enhancing our ability to encourage organizations to produce and maintain trustworthy software***
- ***Reforming the procurement process***
- ***Increasing our investment in education and the big "R" of R&D to improve on our track record of technology transfer***

Example Challenge Discussed in Monterey

- **Problem**: Federal government is not adequately focused on trustworthy software (software-intensive products and systems)
- **Opportunity**: Government could leverage its buying power (~$60B in IT) to influence the trustworthiness of software
- **Recommendations**: (i) Improve specificity of trustworthiness requirements for use by the Federal Government as the acquirer of software; (ii) strengthen OMB A-11 (and similar rules for acquiring IT) and the FARs; and (iii) have NIST provide specific guidance for improving acquisition

cigital

Closing Comments

1. New online community in trustworthy software - www.ieeecommunities.org Let us know if you would like to join.

2. The Monterey workshop identified a series of challenges that the CNSS can more forward on and create solid recommendations for.

3. It is clear that the meaning of “software trustworthiness” is in the eye of the beholder. No definition for software trustworthiness exists that is universally accepted. We still need consensus to move forward.

4. The Monterey meeting was a very successful event; many participants wish to build a community around this topic and meet on a regular basis.