Challenges in the Current Standards and Certification Process

Mark Skall

What is a Standard?
VVSG = Voluntary Standard

In voting: standard = guideline

Voluntary Voting System Guidelines (VVSG)

Voluntary

Use is not mandated by law or regulation

If you decide to use it (claim conformance), then you need to (must) conform to it (adhere to its requirements)

Standard

Established by consensus or authority, and

Prescribes technical requirements to be fulfilled by a product, process or service

Requirement

Criteria, characteristic, behavior, or functionality that a system must do/have

Good Standards are the Key

Goal is correct, reliable software and hardware

Requirements are captured in a standard

Standard needs to be clear, precise, unambiguous, complete, and testable

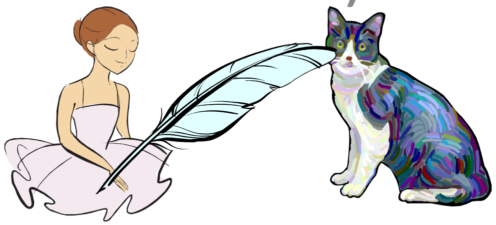
Ideal standard would be defined in a mathematical language – not English – but, it needs to be readable and understandable

English is not Precise

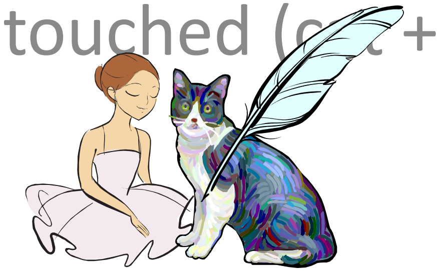
English is not Precise

The girl touched the cat with a feather

(Girl + feather) touched cat



Girl touched (cat + feather)



What makes a good standard?

One that gets used, used correctly and implemented in a consistent manner

One that defines

What/who needs to implement the standard

Normative vs. Informative

What needs to be implemented (Mandatory vs. Optional)

One that is modular with minimal redundancy

One that is adaptable as things change

One that is technology - and design - independent

Type of Requirements

Functional:

Specifies that the object is capable of performing a certain action

e.g., The system shall allow the voter to cast a straight party vote

Performance:

Specifies not only that the object is capable of performing a certain action, but also sets a benchmark for how well it performs.

e.g., The system shall provide visual feedback within .5 seconds when the voter makes or changes a choice within a contest.

Design:

Specifies something about the static structure of the object.

e.g., Any control buttons on a voting system shall be at least 1 inch apart

Independence

Technology independent

Requirements not tied to a specific technology

Design independent

Requirements tell developers what to build, not how to build it

History of Voting System Standards

- Voting industry created first Voting Systems Standard (VSS) - **1990 VSS**
- VSS updated and issued - **2002 VSS**
- 2000 elections generated concerns over voting system integrity, usability, and security
- 2002 Help America Vote Act (HAVA) was passed to address these concerns
- **VVSG 2005 (1.0)** developed by NIST/TGDC/EAC
  - Update of the 2002 VSS
- **VVSG 2.0** sent to EAC by TGDC in 2007
  - Total re-write of the VVSG 2005
  - Has not yet been promulgated
- **VVSG 1.1** out for public review in 2012
  - Integrate some VVSG 2.0 requirements into VVSG 1.0

How Well Have We Done?

- Are requirements clear, precise, unambiguous, complete, and testable
- Do we define
  - What/who needs to implement the standard
  - Normative vs. Informative
  - What needs to be implemented (Mandatory vs. Optional)
- Are requirements technology and design independent?

How Well Have We Done?

- Are requirements clear, precise, unambiguous, complete, and testable

How Well Have We Done?

- Are requirements clear, precise, unambiguous, complete, and testable
  - No, but they can never be

How Well Have We Done?

- Are requirements clear, precise, unambiguous, complete, and testable
  - No, but they can never be
  - We have a process (RFI) to interpret requirements

How Well Have We Done?

- Are Requirements clear, precise, unambiguous, complete, and testable
  - No, but they can never be
- Do we define
  - What/who needs to implement the standard
  - Normative vs. Informative
  - What needs to be implemented

How Well Have We Done?

- Are Requirements clear, precise, unambiguous, complete, and testable
  - No, but they can never be
- Do we define
  - What/who needs to implement the standard
  - Normative vs. Informative
  - What needs to be implemented
    - Yes

How Well Have We Done?

- Are Requirements clear, precise, unambiguous, complete, and testable
  - No, but they can never be
- Do we define
  - What/who needs to implement the standard (Voting Systems, VSTLs)
  - Normative vs. Informative (Requirements vs. Discussion)
  - What needs to be implemented (Mandatory vs. Optional)
    - SHALL - mandatory
    - SHOULD – optional, recommended
    - MAY – optional, permitted

How Well Have We Done?

- Are Requirements clear, precise, unambiguous, complete, and testable
  - No, but they never can be
- Do we define
  - What/who needs to implement the standard (Voting Systems, VSTLs)
  - Normative vs. Informative (Requirements vs. Discussion)
  - What needs to be implemented (Mandatory vs. Optional)
    - SHALL - mandatory
    - SHOULD – optional, recommended
    - MAY – optional, permitted
- Are they technology and design independent?

How Well Have We Done?

- Are Requirements clear, precise, unambiguous, complete, and testable
  - No, but they never can be
- Do we define
  - What/who needs to implement the standard (Voting Systems, VSTLs)
  - Normative vs. Informative (Requirements vs. Discussion)
  - What needs to be implemented (Mandatory vs. Optional)
    - SHALL - mandatory
    - SHOULD – optional, recommended
    - MAY – optional, permitted
- Are they technology and design independent?
  - Not yet

Are Standards Enough?

No

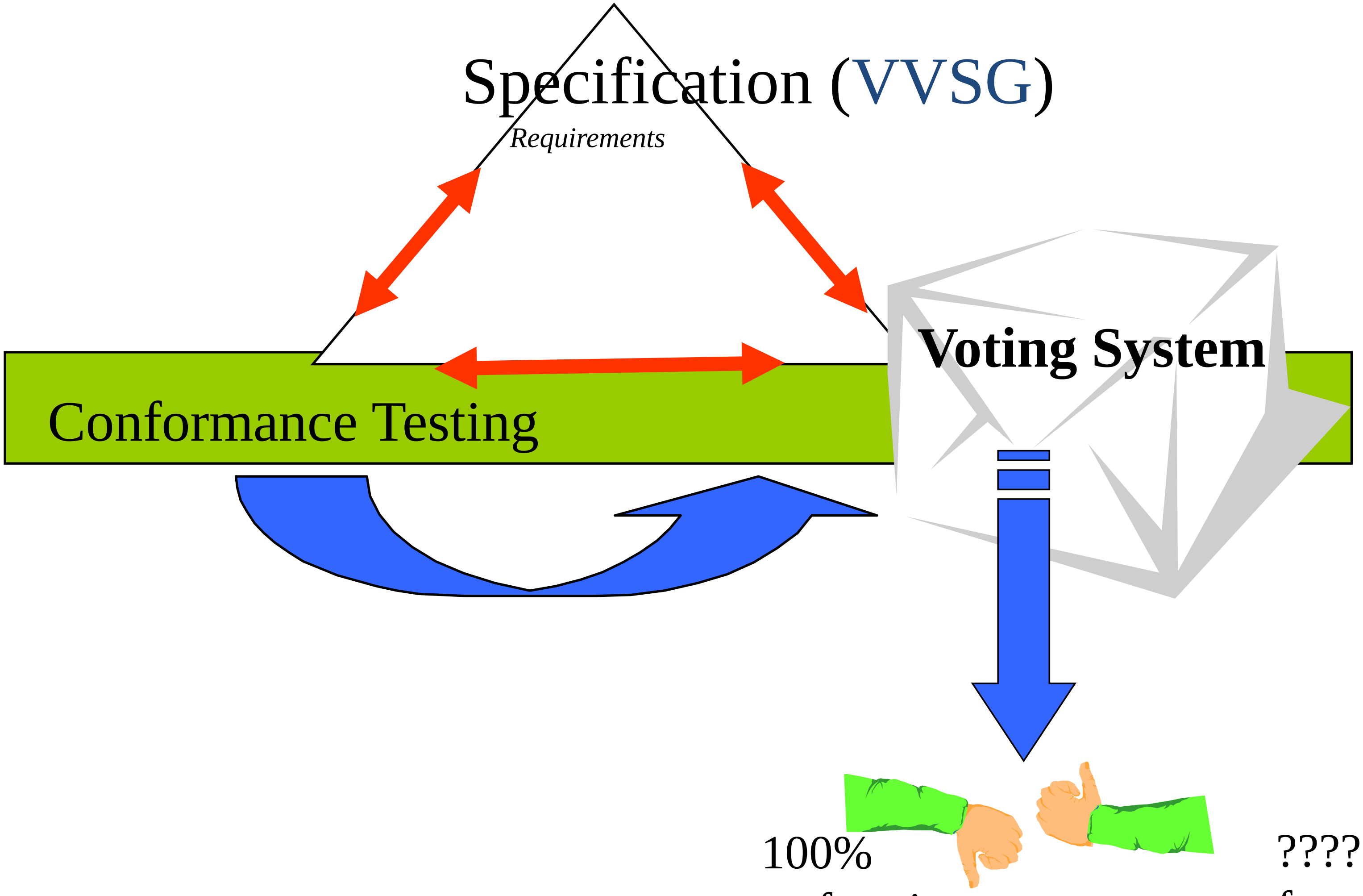
Standards are worthless

Unless they are implemented

Standards are useless

Unless they are implemented correctly

That’s where conformance and



Specification (VVSG)

Requirements

Conformance Testing

Voting System

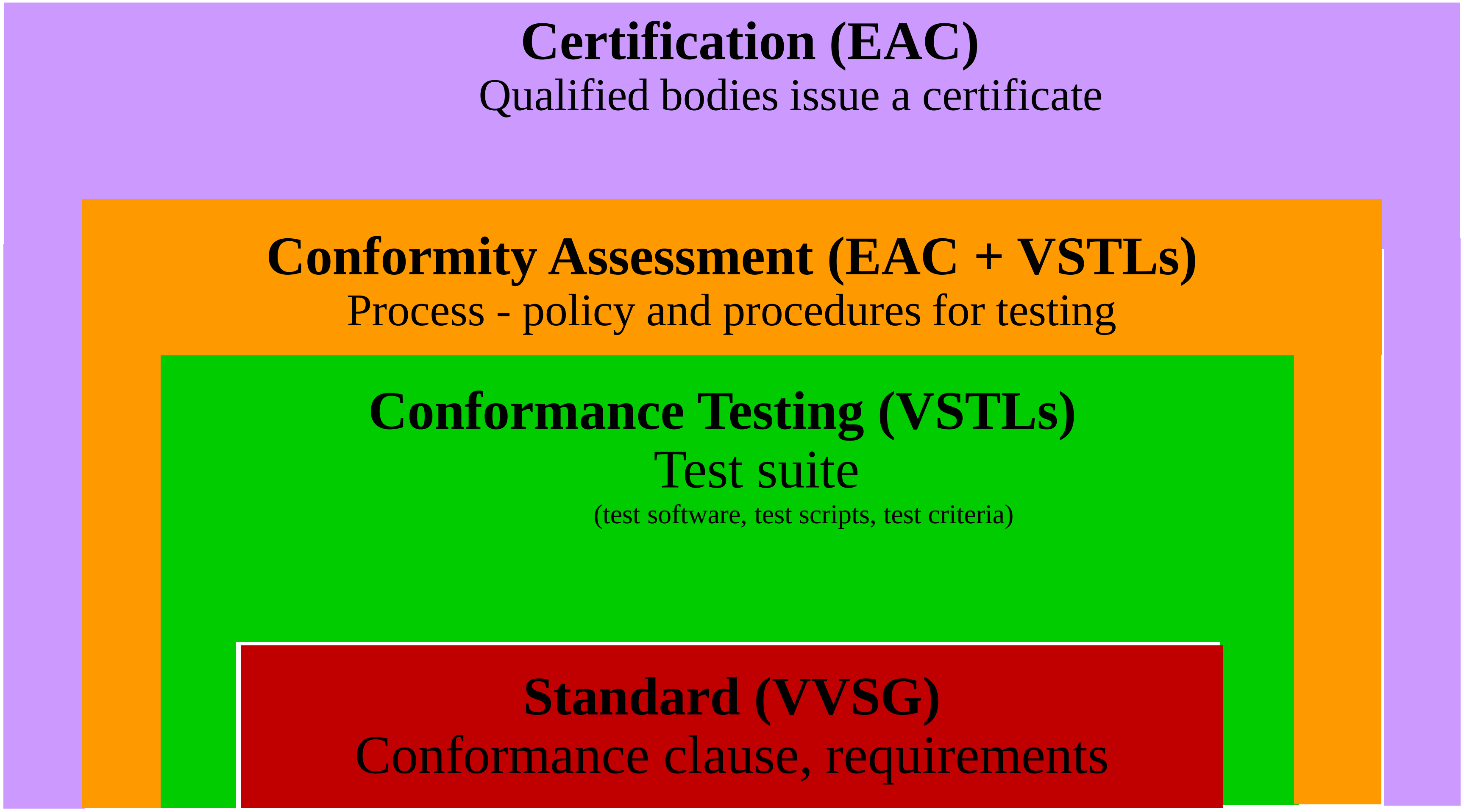
100%
non conforming

????
conforming

Conformance Testing

- Methodology
  - Falsification testing
  - Find errors by means of experimentation
- Outcomes
  - Show presence of errors not their absence
  - Demonstrates non-conformance; can never prove conformance
- Issues
  - How much testing is enough?
  - How can we produce more tests with less resources?
- Early involvement improves quality of software

The Process



Certification (EAC)
Qualified bodies issue a certificate

Conformity Assessment (EAC + VSTLs)
Process - policy and procedures for testing

Conformance Testing (VSTLs)
Test suite
(test software, test scripts, test criteria)

Standard (VVSG)
Conformance clause, requirements

Why is Voting So Difficult?

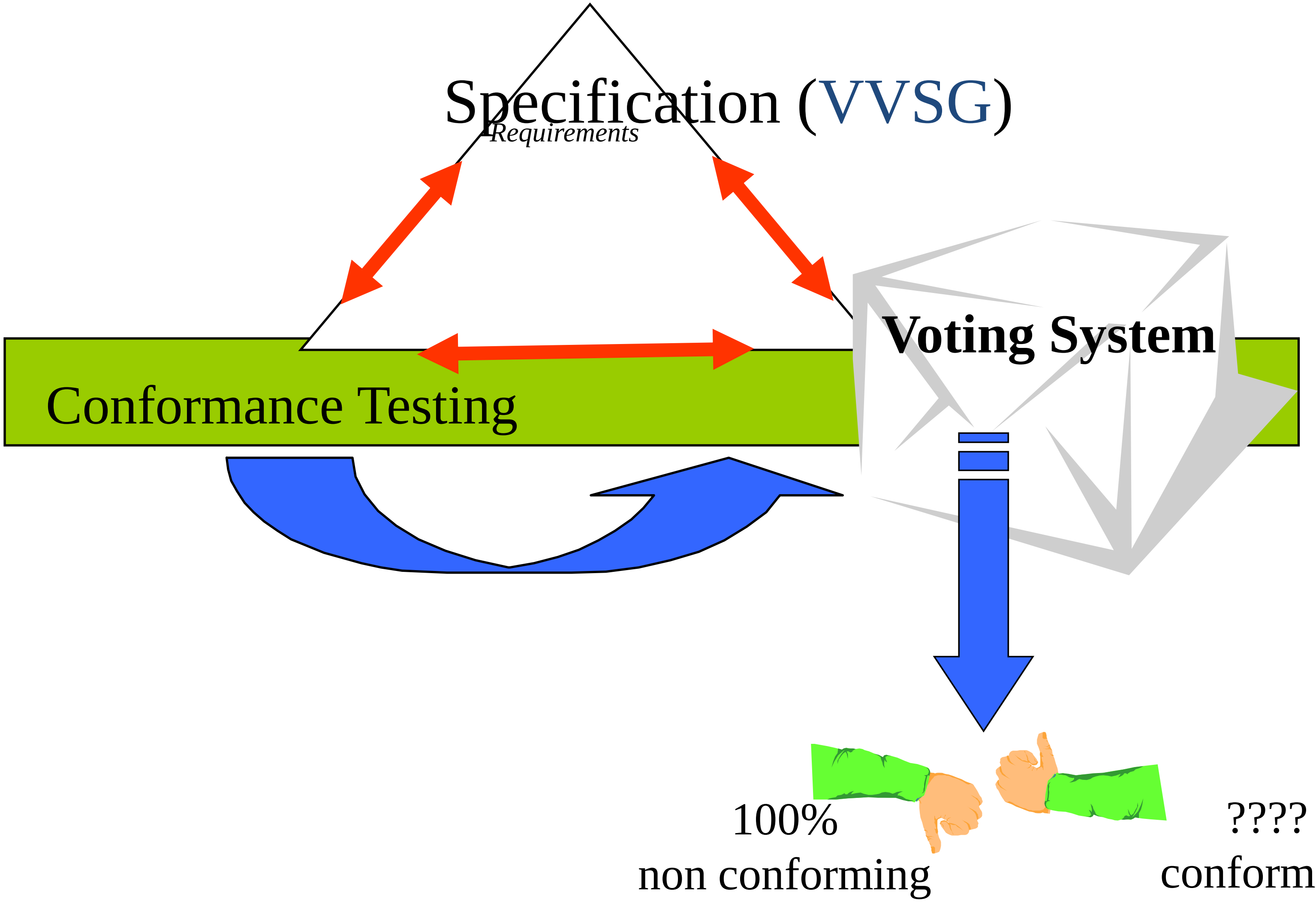
Why is Voting So Difficult?

  - Testing software is difficult enough

Why is Voting So Difficult?

- – Testing software is difficult enough
- – Testing voting systems have their own unique problems

Why is Voting So Difficult?
Generic Issues



Why is Voting So Difficult? Generic Issues

- Can’t measure effectiveness of testing
  - Too many combinations to test exhaustively
  - Even if all the tests are passed we do not know the probability of the voting system being correct (i.e., containing no errors)
  - Very high probability there will still be errors that may show up on election day – just don’t know which or how many

Issues Unique to Voting Systems

Voting is not Rocket Science

Voting is not Rocket Science

- It’s Harder

Why is Voting So Difficult?

Why is Voting So Difficult?

- The Secret Ballot

Why is Voting So Difficult?

- The Secret Ballot
  - Can’t associate the actor with the transaction

Why is Voting So Difficult?

- The Secret Ballot
  - Can’t associate the actor with the transaction
  - Difficult to track problems that have occurred
    - May not even be aware there is a problem

Why is Voting So Difficult?

- The Secret Ballot
  - Can’t associate the actor with the transaction
  - Difficult to track problems that have occurred
    - May not even be aware there is a problem
  - This is the game changer

Why is Voting So Difficult?

- Lack of Resources/Funding
- Compare with mission critical systems
  - Can build redundant systems like in airplanes
  - Can utilize formal methods to specify requirements and then check to see if requirements have been met
  - Can test much more comprehensively
- No loss of life with elections but how much is our democracy worth?

Why is Voting So Difficult?

- Voting Systems going in for certification are not always production ready
  - Manufacturer software development process, testing and Q/A should be at a high level
  - Certification/conformance testing should not be beta testing

Why is Voting So Difficult?

- Voting Systems take a long time to get certified and the process is very expensive and labor-intensive
  - New systems can take from one year to as much as three or four years to get certified

Why is Voting So Difficult?

- Voting Standards are part of the problem
  - Large, monolithic standards
  - Requirements vague or ambiguous
- Unclear requirements lead to lack of uniformity among Test Labs (VSTL)
  - Each lab has their own interpretation of requirements
  - Each Lab has their own tests to test requirements
- Some requirements, like security, can’t be precisely specified, necessitating open-ended (penetration) testing
  - This further erodes uniformity and testing

Why is Voting So Difficult?

- Goal Requirements
  - Requirements that can identify goals but are untestable
  - Requirements that could be tested but testing will be subjective and non-repeatable

Why Goal Requirements?

- Some requirements express a goal to be met by the vendor
- Usually a performance requirement, but without clear performance measures
- Often done to avoid constraining design

Obvious examples

- Instructions SHALL be readable
- The voting machine SHALL provide clear instructions
- The voting process SHALL be designed to minimize cognitive difficulties
  - Testing will be subjective
  - It will be non-repeatable
- VVSG has roughly 20-30 goal level requirements

Possible Solutions

Possible Solutions

- How can we judge how realistic the proposed solution is?
  - Is it feasible?
  - How quickly will it get done?
- We need a metric

Possible Solutions

- Which will come first – Will we solve the problem with the proposed solution or will Matt Masterson become Governor of Ohio?

Possible Solutions

- Problem – The secret ballot

Possible Solutions

- Problem – The secret ballot
- Solution – Abolish the secret ballot

Possible Solutions

- Problem – The secret ballot
- Solution – Abolish the secret ballot
- Which will come first?

Possible Solutions

- Problem – The secret ballot
- Solution – Abolish the secret ballot
- Which will come first?
  - Congratulations Governor Masterson

Possible Solutions

- Problem – Systems take a long time to get certified and the process is very expensive

Possible Solutions

- Problem – Systems take a long time to get certified and the process is very expensive
- Solution – Voting Systems going in for certification will be ready to be tested and certified
  - Manufacturer software development process, testing and Q/A will be at a high level
  - EAC will spend more time checking readiness

Possible Solutions

- Problem – Systems take a long time to get certified and the process is very expensive
- Solution – Voting Systems going in for certification will be ready to be tested and certified
  - Manufacturer software development process, testing and Q/A will be at a high level
  - EAC will spend more time checking readiness
- Which will come first ?

Possible Solutions

- Problem – Systems take a long time to get certified and the process is very expensive
- Solution – Voting Systems going in for certification will be ready to be tested and certified
  - Manufacturer software development process, testing and Q/A will be at a high level
  - EAC will spend more time checking readiness
- Which will come first?

  - Keep your day job, Mr. Masterson – this is already happening

Possible Solutions

- Problem – Voting standards are written in English, which is an inexact language

Possible Solutions

- Problem – Voting standards are written in English, which is an inexact language
- Solution – Write voting standards in a formal or semi-formal (mathematical) language

Possible Solutions

- Problem – Voting standards are written in English, which is an inexact language
- Solution – Write voting standards in a formal or semi-formal (mathematical) language
- Which will come first?

Possible Solutions

- Problem – Voting standards are written in English, which is an inexact language
- Solution – Write voting standards in a formal or semi-formal (mathematical) language
- Which will come first?
  - The Governorship: Voting standards need to be readable by the general public

Possible Solutions

- Problem – Large, monolithic standard

Possible Solutions

- Problem – Large, monolithic standard
- Solution – Create standards with partitions and allow implementations of the partitions to be certified
  - Levels
  - Core plus requirements

Possible Solutions

- Problem – Large, monolithic standard
- Solution – Create standards with partitions and allow implementations of the partitions to be certified
  - Levels
  - Core plus requirements
- Which will come first?

Possible Solutions

- Problem – Large, monolithic standard
- Solution – Create standards with partitions and allow implementations of the partitions to be certified
  - Levels
  - Core plus requirements
- Which will come first?

Not so fast Mr. Masterson – this *could* happen

Possible Solutions

- Problem - Lack of Resources/Funding

Possible Solutions

- Problem - Lack of Resources/Funding
- Solution – Get Congress, or others, to recognize the breadth of the problem and something will be done

Possible Solutions

- Problem - Lack of Resources/Funding
- Solution – Get Congress, or others, to recognize the breadth of the problem and something will be done
- Which will come first?

Possible Solutions

- Problem - Lack of Resources/Funding
- Solution – Get Congress, or others, to recognize the breadth of the problem and something will be done
- Which will come first?
  - Not going to happen even after Mr. Masterson serves two terms as Governor

Possible Solutions

- Problem – Requirements are vague or ambiguous leading to inconsistent interpretation and lack of uniformity among VSTLs

Possible Solutions

- Problem – Requirements are vague or ambiguous leading to inconsistent interpretation and lack of uniformity among VSTLs
- Solution – EAC, NIST and Test Labs develop test assertions that break down the requirements into well-understood, unambiguous chunks

Possible Solutions

- Problem – Requirements are vague or ambiguous leading to inconsistent interpretation and lack of uniformity among VSTLs
- Solution – EAC, NIST and Test Labs develop test assertions that break down the requirements into well-understood, unambiguous chunks
- Which will come first

Possible Solutions

- Problem – Requirements are vague or ambiguous leading to inconsistent interpretation and lack of uniformity among VSTLs
- Solution – EAC, NIST and Test Labs develop test assertions that break down the requirements into well-understood, unambiguous chunks
- Which will come first
  - Find another line of work, Mr. Masterson – this

Testing Requires Unambiguous Requirements

- Need mutual understanding of VVSG requirement among voting system manufacturers, VSTLs and the EAC
- The “devil is in the details” to unambiguously specify requirements
- Test assertions can provide that mutual understanding among the EAC, NIST, manufacturers and VSTLs

Assertion-Based Testing Framework for Voting

- An effort to provide a reference set of assertions that are complete, unambiguous, and:
  - *Provide a uniform testing reference* for VSTLs and voting system manufacturers, across all testing domains (security, usability, software requirements, performance, etc.)
  - *Provide a "bridge"* between the VVSG requirements and test suites (manufacturer's, VSTL's or NIST's)
  - *Provide testable expressions* (assertions) that more succinctly and practically describe

Assertion-Based Testing Framework for Voting

- This is a team effort among NIST, EAC and VSTLs
  - Everyone has to agree before test assertion is finalized
  - Made available to manufacturers for their comments
  - Decisions are somewhat subjective but better to interpret these one time by a consensus than having VSTLs interpret them unilaterally and inconsistently

Example of a Test Assertion

- VVSG Requirement – Each module shall be mnemonically named
  - Test Assertion - If a class, interface or callable unit is declared, its intrinsic purpose can be determined by its name.

Test Suite Development

- NIST has developed a set of public test suites to be used in EAC’s Testing and Certification Program
- The test suites address all requirements in the VVSG 2.0
  - Tests are thus available for the VVSG 2.0 requirements that have been back ported to 1.1
- Use of the public test suites by test labs will produce consistent results and promote transparency of the testing process

To Recap

- Voting is hard

To Recap

- Voting is hard
- We have to live with many of the constraints
  - Uncertainty of conformance testing
  - The secret ballot
  - Scarcity of resources/funding

To Recap

- Voting is hard
- We have to live with many of the constraints
  - Uncertainty of conformance testing
  - The secret ballot
  - Scarcity of resources/funding
- For the rest, we’re making progress

To Recap

- Voting is hard
- We have to live with many of the constraints
  - Uncertainty of conformance testing
  - The secret ballot
  - Scarcity of resources/funding
- For the rest, we’re making progress
- Matt Masterson *will* become Governor of Ohio