Improving U.S. Voting Systems

- NIST activities supporting the Help America Vote Act

NIST National Institute of Standards and Technology

Next VVSG Training

VVSG Overview Module

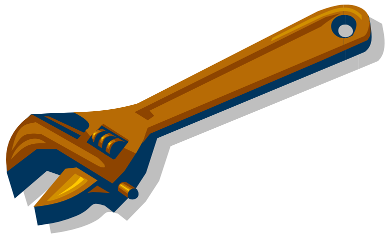
December 2007

John P. Wack
National Institute of Standards and Technology
john.wack@nist.gov

NIST National Institute of Standards and Technology

Goals of this module

- To give you the tools you need to understand the document
- For you to understand some of the background that went into the document structure and material
- For you to help other election officials and the public better understand the VVSG
- For you to make the best comments possible during the public reviews



Contents

1. Overview of the VVSG document and rationale behind its structure
2. An initial walk through the material
3. The Conformance Clause
4. Some setup for the following presentations

1: Overview of the VVSG document and rationale behind its structure

Scope

- The VVSG addresses all new equipment
- But, as much as possible, the VVSG basically expands upon the many good things already in VVSG 2005 (and the 2002 VSS)
  - If something wasn't broken, the TGDC didn't try to fix it
  - Many of the new requirements make old requirements in previous guidelines more specific and testable
- To the extent possible, consideration was given to expense before adding new requirements that would change hardware

The VVSG audience

- The primary audience must be vendors and test labs
- At the same time, it must be understandable to people who use the equipment and the public at large
  - The TGDC recognized the tension between preciseness and plain language
  - Attempts to reduce ambiguity doesn't always result in greater understandability for less technical audiences
  - The chosen format and language is intended to promote usability and understandability for all
  - A companion document is being written for less technical audiences

VVSG structural decisions

- The VVSG's structure is critical to its successful usage
  - One needs a highly usable document from which to base decisions
  - Wonderful material, poorly organized, won't necessarily be effective if people can't read it or find what they need
- The TGDC viewed the VVSG as a tool, akin to the carpenter's workbench, for building better voting systems
- Much effort was put into organization, look, and feel of the document

- The VVSG is also meant to be used as an electronic document, with numerous hypertext links and other features

Improved precision and durability

- The new structure of the VVSG improves upon precision and durability issues with previous guidelines
- It has a foundation that accommodates updates and additions; impacts to other parts of are minimized

- It is now structured more akin to ISO & W3 standards, information is more organized and logically grouped
- It adheres strictly to a glossary, ambiguity of language is reduced, requirements are more precise
- Requirements are scoped precisely to devices and testing approaches
- Fundamentally different types of requirements are organized into different parts

The glossary

- A well-understood vocabulary is critical to promoting precision and common understanding
- The scope of the VVSG glossary is specific to the VVSG, however:
  - Many terms in common usage have slightly different meanings to different localities; this presents a big problem when everyone needs to be on the 'same page'
  - The TGDC tried to use commonly-accepted terminology and definitions, but they may not jive always with local usage
  - This is okay to an extent as long as everyone understands the terms
  - This is why glossary terms are hyperlinked to their definitions

2: An initial walk-thru of the VVSG

VVSG Parts

- Requirements in the VVSG are organized into different parts (sections) to make the document more usable
- Akin somewhat to previous guidelines (e.g., Volumes 1 and 2 of VVSG 2005)
- Part 1: Rules of conformance and all device requirements
- Part 2: TDP and user documentation requirements
- Part 3: Testing related information and requirements
- Chapter 1 in each part: changes from VVSG 2005

Overview of Part 1

- Intended for vendors and test labs
- Structure resembles organization of TGDC subcommittees
  - Human factors
  - Security
  - Core requirements
- Human factors represents requirements that most directly impact voters
- Security material deals with SI, IVVR, and building-block security requirements
- Core requirements chapters deal with reliability, accuracy, everything else after human factors and security

Overview of Part 2

- Intended for vendors and test labs
- Deals primarily with the Technical Data Package (TDP) that a vendor submits to a test lab
  - Previous guidelines did not make clear what material is required in the TDP
  - Part 2 now contains all TDP requirements
- User documentation is part of the TDP

Overview of Part 3

- Intended primarily for test labs
- Informative material on
  - Conformity assessment process
  - Testing approaches
- Contains requirements for test labs relating to
  - Pre-test preparations
  - How voting systems are to be submitted
  - The build environment
  - Software/Hardware testing
  - OEVT ...

3: The Conformance Clause

Chapter 2: Conformance Clause

- It’s not a clause; it’s just called that
- Discusses overall aspects of what constitutes conformance to the VVSG
- Useful for the vendor who needs to understand what constitutes conformance

Foundation of the VVSG

- By necessity, the CC explains foundational, structural aspects of the VVSG
  - How and why requirements are structured
  - Meaning of certain language
  - Conformance to the VVSG
  - System and device classes
  - Extensions
  - Software independence

2.2: Language

- Normative – Requirements text, contains "*SHALL*" statements
- Informative – everything else ("must" instead of "*SHALL*" used)
- Exceptions or Fuzziness:
  - A requirement may mandate use of information in a table, thus the table is normative
  - A requirement's description field may add explanation to the requirement; while not normative per se; the explanation is intended to be used by the test labs and vendors

2.1: Requirements

- Requirement structure
- Requirement fields
  - Extra info on the *Applies to:* field
- Parent and sub-requirements

Requirement structure

- Requirement title – for use in references to requirements via tables or future DBs
- Requirement sub-text – the normative requirement language, blue
- *Applies to:* which voting (almost always) device class this requirement applies to (voting system class, otherwise)
- *Test reference:* what test approach(es) will be used to test the requirement, refers to corresponding material in Part 3
- Discussion - (optional) informative discussion about the requirement, further explanation, things we'd like you to know
- *Source:* (optional) this requirement's genesis or forebears

Which fields are used where?

- Part 1: Equipment Requirements
  - Optional: *Source:*
- Part 2: Documentation Requirements
  - *Test reference:* not used
  - Assumption is "all requirements tested by Part 3 Chapter 4 Documentation and Design Reviews"
- Part 3: Testing Requirements
  - *Test reference:* not used
  - Test reference is implied by the requirement and its context in Part 3

Applies to: field

- Almost always a device class
- Otherwise a system class if requirement refers to voting variations at the voting system or device level
- A sub-requirement can narrow the scope of a parent:
  - If the parent applies to a super-class, the sub can apply to a sub-class of the super-class
  - e.g., if *Applies to: tabulator* in parent, a sub could use *Applies to: PCOS*
  - If the sub doesn't narrow the scope, the *Applies to:* field isn't required

Parent and Sub-requirements

- Parent requirements have sub-requirements
- Sub-requirements generally serve to ...
  - Add more specificity to the parent and make it directly testable
  - Turn a “goal” parent into directly testable sub-requirements
  - Narrow the scope of the parent
  - Make readable what would otherwise be a difficult to read parent

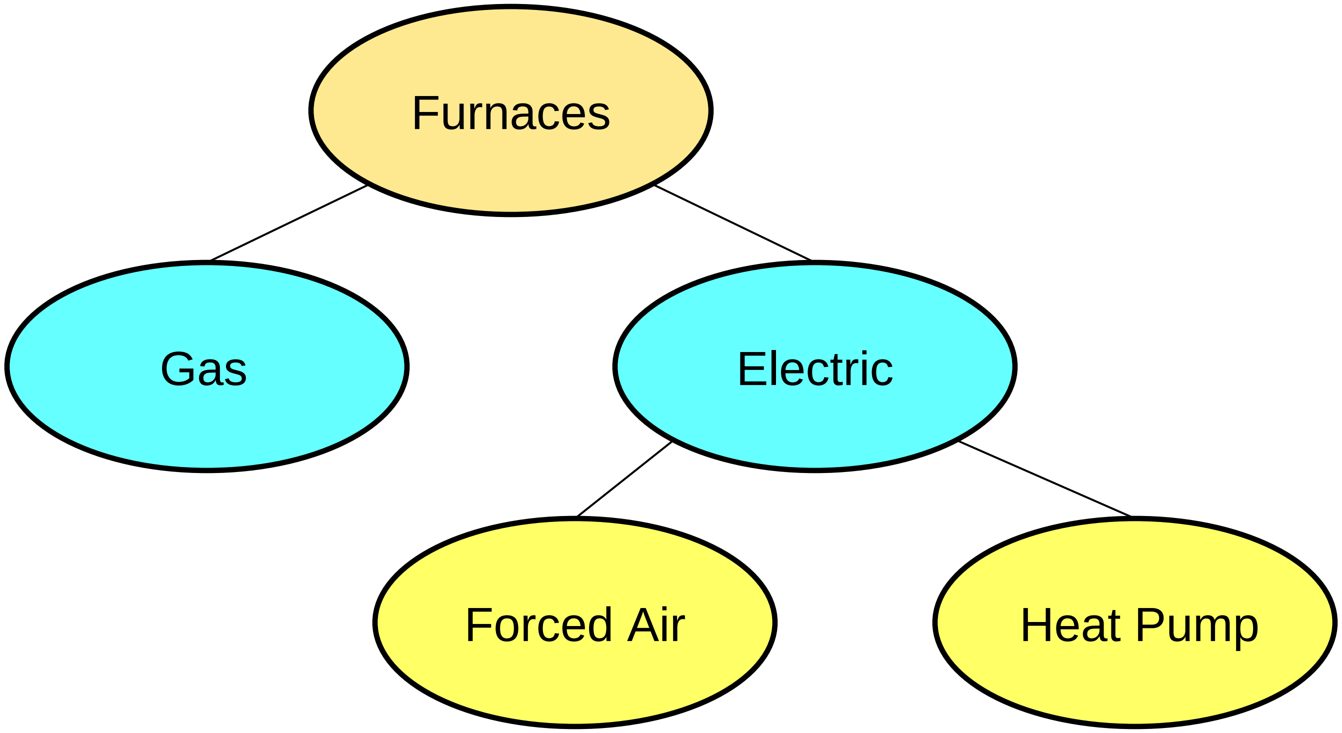
2.5: Class structure

- Classes look hard to understand but they mostly aren't

"it's easier than brain surgery…"

- Think of them mostly as device specifications that get more specific as one gets deeper in the class structure
- Certain basic rules for inheritance apply
- Classes are covered in more detail in core requirements module

Class structures are common



Furnaces

Gas

Electric

Forced Air

Heat Pump

Life without class structures

- Lots of repetition of slightly different requirements
- A much more difficult document to maintain
- E.g., a typical chapter in Part 1 might look like:
  - Requirements for VVPAT and Op scan
  - Requirements just for Op scan
  - Requirements for EBM and VVPAT
  - Requirements just for VVPAT
  - Requirements just for EBM
  - et cetera ad nauseum...

System and Device classes

- Requirements mostly apply to device classes
- System classes used for requirements dealing primarily with support of voting variations (Part 1 Chapter 6 and 7)
- Set math in section 2.5.4 intended primarily for labs and vendors

- These distinctions will be covered in more detail in core requirements module

Interpreting Applies to: fields

Table 1-1 Examples for *Applies to:* fields

APPLIES TO:	MEANING
Vote-capture device	Applies to all Vote-capture devices.
DRE, Activation device	Applies to all DREs and all Activation devices.
DRE ^ Activation device	Applies only to a DRE that is also an Activation device.
Voting device	Applies to all voting devices (voting device is the superclass of all voting device classes).
Voting system	Applies to the voting system as a whole; might be satisfied by a single device or by multiple devices working together.

2.3 thru 2.6: Conformance

- A voting system conforms to the VVSG if all stated requirements that apply are met (2.3)
  - It cannot partially conform
  - Individual voting devices are tested only as part of a voting system
- The implementation statement (2.4-A) documents the requirements implemented (as well as other features and functionality)
  - Also documents classes implemented (2.5)
- Any extensions cannot break or relax requirements that would otherwise apply (2.6)

2.7: Software Independence

- Based on difficulty of testing voting system software for correctness
  - Intentionally-hidden code could be very difficult for a test lab to find
  - Bugs are inevitable and difficult to find
  - Updates to voting system software can cause unforeseen problems
  - The more one tests, the higher the costs

SI Concept

- It can’t be possible to cause an undetectable change in election results due to an error, fault, fraud in the software
- Audits of the electronic CVRs don’t necessarily rely on the software having correctly recorded the voter’s intent, there is recourse
- In other words, sound audits will detect problems that otherwise couldn’t reliably be detected if one must trust that the software was working correctly

SI -> Independent Audits

- STS believes that well-engineered equipment requires capability for independent audits
- DRE approach relies on trusting software as well as uniformly applying effective procedures
- STS could not write requirements to make DRE approach secure – too complex
  - Complexity can be the enemy of security
  - Procedures, no matter how effective and uniform, cannot make up for weaker security

Voting systems that are SI

- SI does not equate always to PAPER
- Includes IVVR (covered in more detail in security modules)
- Innovation Class submissions
- Promising innovative approaches in research include:
  - Cryptographic protocols
  - Witness

Why not 2005's IV?

- VVSG 2005 contained guidelines for Independent Verification (IV or IDV) voting systems
- Permitted an all electronic-record approach in which two independent systems could provide security
  - Noted example was "Frog" protocol
  - No commercial approaches at this point, however
- TGDC deemed that testable performance requirements for IV are premature at this point
- IV guidelines in VVSG 2005 still useful for researchers

2.7.1: SI-IVVR Requirements

- SI is required in VVSG, either through IVVR systems or SI systems submitted via Innovation Class
- IVVR systems must include an IVVR vote-capture device, e.g.,
  - VVPAT
  - Op scan

2.7.2: Innovation Class

- TGDC deemed testable performance requirements for non-IVVR SI systems are still premature
  - VVSG 2005 included end-end cryptographic guidelines, but specific design requirements would constrain approaches under research
- But, it wanted a standards-based, open approach to reviewing innovations that would work within framework of the VVSG
- Thus, TGDC decided to include only basic IC submission requirements in the next VVSG
- It urged the EAC to continue to develop and publish detailed plans and specific procedures for an IC program, with assistance from NIST

IC submission requirements

- Innovative submission treated as a new device class to be implemented
  - Approach must follow class rules
  - Meet other applicable VVSG requirements
- Its innovativeness must be justified
- New applicable requirements and test methods must be identified

IC program development

- TGDC urges IC program to deal with reviews, admissions, and rejections
- Additional review criteria needed; 2005 IV requirements may be useful
- Submissions may require expanded OEVT, other new types of testing
- Will be experimental, will have growing pains, etc.

4: Some setup for the following modules

Parts 2 and 3 material

- Presentations will mainly focus on Part 1
- Material from Parts 2 and 3 is subsumed somewhat into those presentations
- If at any time you get lost in understanding structural issues or where material is located, please ask

What isn't in the VVSG

- Some items in the VVSG expect that external parties will further develop procedures or operational programs, e.g.,
  - Handling of digital certificates for voting systems
  - The Innovation Class
  - Standards maintenance
- Presenters of other modules may deal with these items but don't have all the answers at this point in time

Done with the overview