Core Requirements and Testing Part 1

Alan Goldfine

Computer Scientist

Contents of CRT Presentation

- Electrical/Electromagnetic Requirements
- Reliability (including QA/CM)
- Accuracy and Reliability Benchmarks, Metrics, and Test Methods
- COTS
- Conformity Assessment, Scope of VVSG testing
- Coding Conventions and Logic Verification
- California Volume Reliability Testing Protocol
- Discussion

Electrical/Electromagnetic Requirements

- Electromagnetic Requirements
  - Reviewed by NIST-Boulder experts
- Electrical Requirements
  - Reviewed by NIST-Gaithersburg experts

Reliability

Two aspects:

- How can we measure the reliability of a given voting system?
- What steps can be taken to ensure more reliable voting systems?

Measuring Reliability

- Very informally, the current (MTBF) approach can be described as follows:
  - test the voting system, treated as a self-contained black box
  - note the number of system failures
  - calculate, according to appropriate statistical techniques, the likelihood that the voting system will fail during a period of time (the MTBF metric)

Measuring Reliability

  - if the results are acceptable, then the system passes the test

- The current approach (both the current test methods and the parameters) has drawn criticism

Measuring Reliability

- An approach has been discussed that would integrate the testing for system reliability into the test method proposed for system accuracy
- This approach will be discussed in the Part 2 of the CRT presentation

Ensuring Reliability

- A research effort has been initiated to investigate requirements for voting systems that would assure maximum system reliability in a cost-effective manner
- Two research papers:
  - http://vote.nist.gov/Reliability_Reqs_Metrics_Certification20061019.pdf
  - http://vote.nist.gov/QualityConfigMgtReqs-20061120.pdf

Ensuring Reliability

- Key idea—you guarantee reliability not so much by testing a system for reliability as by building it into the design of the system in the first place

Ensuring Reliability

- Some of the ideas emerging from the research:
  - failures can be prevented through careful design and testing
  - voting systems should be designed in a modular fashion, with well-specified inputs and outputs
  - systems should be capable of using EML for data interchange

Ensuring Reliability

- system software must be transparent, functionally verifiable, and not contain code that is not used
- systems should contain a "verification unit" that ensures that a system about to be used is the same as the one that was certified
- ongoing gathering and analysis of results from the field must be a mandatory part of voting system operation

Ensuring Reliability

- An approach has been discussed that would require voting system vendors to implement a quality assurance program that is conformant, within the appropriate scope of operation, to the ISO 9000/9001 standard

Quality Assurance

- In the current VVSG
  - vendors can design and implement any program that ensures that “the design, workmanship, and performance programs are achieved in all delivered systems and components.”
  - the QA program is the responsibility of the vendor, who is required to provide test data and test reports as part of the testing process

Quality Assurance

- However, the VVSG
  - currently specifies QA guidelines that might not be tight enough
  - does not make use of any generally accepted standard that QA programs would be required to comply with, relying instead on a vendor developed program

Quality Assurance

– essentially provides for the review of the vendor program at testing time, i.e., only after the quality program has already run its course

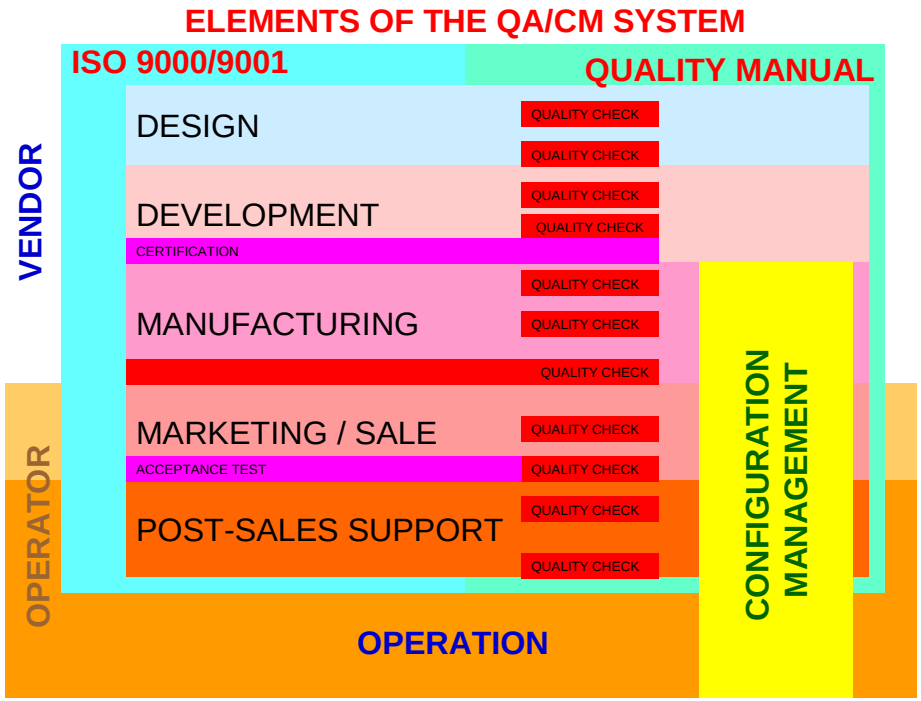
Quality Assurance

- ISO 9000/9001 is the recognized QA standard. It
  - has been successfully applied to product development in many industries
  - is relevant and applicable to the development of voting systems
  - helps ensure that quality is built into voting systems from the start, and throughout development

Quality Assurance

- ISO 9000/9001 standard itself defines requirements in generic terms
- As part of the process, a quality manual is developed that details the quality process for a vendor within the ISO 9000/9001 framework
- VVSG must contain explicit requirements for the quality manual, to ensure a meaningful program

Quality Assurance



From http://vote.nist.gov/QualityConfigMgtReqs-20061120.pdf

Quality Assurance

- Choices in adopting ISO 9000/9001
  a) formal certification through a third-party audit performed by an organization accredited by the ANSI National Accreditation Board provides—a review that is expert and rigorous enough to be relied upon by testing labs and the EAC
  b) vendor self-declaration of conformance
  c) EAC decides between a) and b) either in general or on a case-by-case basis