Core Requirements Overview (Part IV)

October 15-17, 2007

David Flater
National Institute of Standards and Technology
dflater@nist.gov

6.4 Workmanship

- 6.4.1 Software engineering practices
- 6.4.2 Quality assurance and configuration management
- 6.4.3 General build quality
- 6.4.4 Durability
- 6.4.5 Maintainability
- 6.4.6 Temperature and humidity
- 6.4.7 Equipment transportation and storage

6.4.1 Software engineering practices

- 6.4.1.1 Scope
- 6.4.1.2 Selection of programming languages
- 6.4.1.3 Selection of general coding conventions
- 6.4.1.4 Software modularity and programming
- 6.4.1.5 Structured programming
- 6.4.1.6 Comments
- 6.4.1.7 Executable code and data integrity
- 6.4.1.8 Error checking
- 6.4.1.9 Recovery

Executive summary

- Manufacturers are expected to use current best practices for software engineering
  - “Published” and “credible” coding conventions
  - Three year rule and reassessments
- Worst practices are prohibited
  - I.e., practices that are known risk factors for latent software faults and unverifiable code
- Defensive programming is required
- Use of state-of-the-art programming languages and standards facilitates compliance

Executive summary: Q & A

- Chris Thomas, Michigan
- David Flater, NIST
- Britt Williams, TGDC- NASED

Executive summary (Continued)

- Worst practices are prohibited
  - I.e., practices that are known risk factors for latent software faults and unverifiable code
- Defensive programming is required
- Use of state-of-the-art programming languages and standards facilitates compliance

Executive summary: Q & A (Continued)

- Wendy Noren, Boone County, Missouri
- David Flater, NIST
- Britt Williams, TGDC- NASED
- Brian Hancock, EAC
- John Lindback, Oregon

Executive summary (Continued)

- Defensive programming is required
- Use of state-of-the-art programming languages and standards facilitates compliance

Executive summary: Q & A (Continued)

- Jim Dickson, EAC Board of Advisors
- David Flater, NIST
- Sharon Laskowski, NIST
- Mary Herrera, New Mexico

Executive summary (Continued)

- Use of state-of-the-art programming languages and standards facilitates compliance

Impact of changes

- Resolved controversy over prescriptive requirements on programming style
- More flexibility for manufacturers
- Pressure to migrate to state-of-the-art programming languages and standards
- Should get more reliable, higher integrity software
- Costs
  - Legacy code must be cleaned up and reinforced to meet the same requirements
  - More experience and judgment required of test labs

Terms

- COTS: includes shrink-wrapped commercial software and analogous open-source packages
  - General-purpose
  - Widely used
  - Unmodified
- Application logic: logic from any source that is specific to the voting system, with the exception of border logic
- Border logic: “glue code”
- Third-party logic: neither application logic nor COTS
  - So-called “modified COTS”
  - Source code generated by a COTS package

“COTS exemption” busted

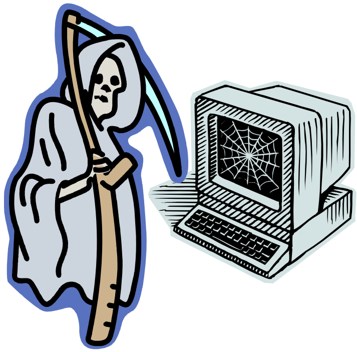
Categories	Level of scrutiny	Tested?	Source code/data required?	Coding standards enforced?	Shown to be correct?
COTS	Black box	Yes	No	No	No
Third-party logic, border logic, configuration data	Clear box	Yes	Yes	No	No
Application logic	Coding standards	Yes	Yes	Yes	No
Core logic	Logic verification	Yes	Yes	Yes	Yes

COTs Q & A

- Nikki Trella, Maryland
- David Flater, NIST
- Lynne Bailey, Georgia
- Doug Lewis, The Election Center

6.5 Archival[ness] requirements

- Records last at least 22 months in temperatures up to 40 °C and humidity up to 85 %



Related requirements

- Part 2 Req. 4.4.8-C Operations manual, procedures to ensure archivalness
  - The manufacturer SHALL detail the care and handling precautions necessary for removable media and records to last 22 months etc.
- Part 3 Req. 4.1-B Review of COTS suppliers' specifications
  - Test lab shall verify that the media are not being used out-of-spec

Impact of changes (archivalness)

- Responsive to complaints about thermal paper going off
- Ambient conditions specified
  - End users should not have to resort to extreme measures to preserve records for the statutory period
- More test lab scrutiny of data sheets for media used
  - Actually supposed to last 22 months in ambient conditions