

# **EAC Voting System Test Laboratory Discussion of TGDC Draft VVSG**

**March 19, 2008  
9:00am – 2:00pm**

**Hyatt Regency Denver  
650 15<sup>th</sup> Street  
Denver, CO 80202**

## **Answers to Discussion Questions**

Prepared by:

**SysTest Labs Incorporated**

**EAC VSTL 0701**



March 17, 2008

As a VSTL, our interest in the new VVSG is twofold. First and foremost, we look to the VVSG for clear and unambiguous guidance on our review, assessment and test activities required to determine whether or not a voting system meets the applicable VVSG requirements. The VVSG must be structured and worded in a fashion that facilitates a thorough understanding and promotes ease of implementation of the requirements, processes, methods, and documentation necessary for a VSTL to provide certification testing of a voting system. Secondly, the VVSG must present the requirements for voting system equipment, software and documentation in a clear and unambiguous manner so that, through our testing, we can determine if a Manufacturer and its system have met each and every applicable requirement defined in the VVSG. It is clear that the new VVSG is far more detailed and precise than its predecessors and represents a significant effort towards improvement over both the 2002 VSS and the 2005 VVSG. However, in its present form, there are still many requirements that are either poorly defined, undefined or difficult to understand, there are test methods that focus on theory and have not been explicitly defined, and the VVSG in and of itself is repetitive, highly technical in nature, and could be viewed as intimidating to non-technical individuals. We are very confident that, after careful study and Quality System process updates and improvements by our test engineers, our test processes, methods, etc. will be effective in testing to determine if a voting system meets the requirements defined in the new VVSG. However, we are hopeful that the time remaining in the public comment period will be used to improve the clarity of the requirements, soften the intimidation factor and explicitly define all required test methods.

1. The 2005 VVSG states one of the goals for the next iteration of the VVSG as being to create performance guidelines that promote innovation rather than design orientated guidelines that limits design choices. Do you think this document achieves that goal? Do you view performance guidelines as sufficiently testable?

We assume that the Innovation Class approach proposed by the TGDC will allow for more extensive opportunities for innovation by a Manufacturer. The goal of the Innovation Class clearly states that it is designed to permit a wide variety of new types of voting systems, either anticipated or unanticipated. We have observed that the current environment for development of voting systems seems to discourage innovation and the pendulum concerning voting system design has swung to the more traditional and less controversial designs for voting systems. We firmly believe that EAC adoption of the Innovation Class proposal will bring some balance to the industry and may result in new ways to conduct and vote elections that will promote voter confidence and meet the needs of election officials.

Regarding the question of whether or not the performance guidelines limit the design choices, one conclusion that we have reached from our review and assessment of what we believe to be the more constraining requirements specified in the new VVSG are that these seem to be directed at existing voting systems that have historically been considered (but not necessarily proven) to be more vulnerable. There are many instances of requirements in the new VVSG that will ultimately result in limiting the

choices for design and implementation. It is difficult to ascertain if the intent was to create a more design oriented set of requirements or if the process of refining the requirements to further ensure that voting systems are accurate, reliable, secure, usable, accessible, and testable has resulted in a natural limitation. Regardless, we believe that the new VVSG has established a very comprehensive and complete set of performance guidelines for the design, development and implementation of voting systems.

While SysTest Labs, has identified a number of items that will be included in our feedback to both the TGDC and the EAC for clarification, correction, and interpretation, we believe that, through a closed loop feedback process, the performance guidelines can be made sufficiently testable.

2. How can innovative systems be evaluated for purposes of certification? If the EAC were to undertake creating an innovation class what suggestions would you make regarding the testing of innovative or new technologies?

Testing innovative or new technologies under the EAC program could take the form of what is referred to as a Delta Certification, testing and certification of a voting system with new or upgraded components. The initial focus of testing would be on the new technology and/or innovation as a separate and distinct component ensuring that it meets the applicable VVSG requirements. It would be anticipated that this initial testing focus would be highly iterative, with a great deal of interaction with the Manufacturer addressing and fixing “discrepancies” and a great deal of interaction with the EAC (or the EAC’s Innovative Class Panel) addressing requests for interpretation. Once a new technology has successfully passed this series of rigorous tests and evaluations, it would have to be incorporated into the voting system as a whole. Assuming that the voting system has been previously certified under the EAC program, a subset of tests, including end-to-end and OEVT, would be executed to ensure that the voting system continues to meet all applicable requirements in the VVSG. If the voting system has not been previously certified by the EAC, then a full certification test engagement would be required.

3. Is Open Ended Vulnerability Testing (OEVT), as presented in the proposed guidelines, feasible in a conformance assessment process? What advantages or disadvantages do you see with OEVT? If the EAC were to require OEVT how could it best be included into the EAC’s Testing and Certification Program?

**3.1 SysTest Labs believes that OEVT, as presented in the proposed guidelines, will be a significant help to the EAC, States and Counties in improving voter confidence in the use of voting systems in the election process. We are confident that VSTLs will be able to implement the changes to our processes and additions to our staff that come with the proposed OEVT guidelines. However, we feel that there will be significant challenges to ongoing management of a certification test engagement. While identification of “architecture, design and implementation flaws that have crept into a voting system which may not be detected using systematic functional, reliability, and security testing and can be exploited to change the outcome of an election, can**

provide erroneous results for an election, can cause denial of service, can compromise secrecy of vote, or can compromise of security audit log<sup>1</sup>”, should be a priority for all VSTLs, changes to a voting system’s architecture and design during certification testing will create significant delays in the certification test process. This statement is not intended to argue against OEVT, but to point out the challenges the EAC will have in trying to get systems certified in a timely manner.

For many years, the software development industry has identified the cost, in time and money, of identifying discrepancies in software at the various stages of a Software Development Life Cycle (SDLC) and that discrepancies can cost as much as 1000 times more if discovered late in the SDLC. Discrepancies identified during OEVT that require a change to the system’s architecture and design will create a ripple effect in the entire certification test process and test schedule that impacts the Manufacturer, the VSTL, the EAC, and the end customers. Significant unexpected delays will result that effect a County’s ability to meet their ever changing requirements and will add costs to the VSTL which are passed on to the Manufacturer and subsequently passed on to the end customers.

Conformance assessment is defined in the VVSG as a “demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”. We believe that the intent of EAC’s program for certification of voting systems is intended to be a conformance assessment. Assessing whether or not a voting system’s architecture and design has flaws as defined above should be performed during the SDLC. This type of activity is referred to as independent verification and validation<sup>2</sup> (IV&V). IV&V has been successfully used in many federal and state programs where development and implementation of critical systems has required the level of testing and assurance that is required by the EAC and the general public. IV&V is performed throughout the SDLC for the system so as to both ensure that the end result meets all requirements and to minimize the time required. The question that SysTest Labs poses to the TGDC and the EAC is, how can OEVT be implemented earlier in the process to help mitigate the impact to certification testing schedules? Should an IV&V approach be used, where the VSTL is engaged much earlier in the Manufacturer’s SDLC process, or is the risk to the time required completing certification sufficiently low enough to incorporate OEVT (and other architecture and design assessment activities) into the EAC’s certification program?

**3.2** A second challenge that is posed by open ended testing is that, open ended testing is essentially another name for what the software testing community refers to as ad hoc testing where the requirements for testing are left to the tester or test team and not necessarily driven by any form of specified requirement or design. Ad hoc testing as well as open ended testing are based on experience, either gained individually or though public forums. Ad hoc or open ended testing poses unique

---

<sup>1</sup> *Open Ended Vulnerability Testing for Software Independent Voting Systems*, National Institute of Standards and Technology, May 16, 2007, Version 1.3

<sup>2</sup> IEEE Std 1012-2004

challenges to the test team as well as development organization. Challenges to the VSTL's OEVT test team comes in defining when testing ends. Open ended is just that, open ended. Although a plan will be developed by the OEVT Team that will initially guide the team through their activities, the time and extent of testing can and will most likely get extended with every new test and discovery. The challenge to the Manufacturer will come in the form of trying to estimate the cost impact, in both time and dollars, on the certification test schedule so that they can communicate (1) to their end customers on what a likely completion date for certification will be and (2) their executive management on what the cost of certification will be for budgeting purposes.

**3.3 Requiring voting system Manufacturers to modify a voting system based on OEVT results that are not tied to a specific standard in the VVSG poses a challenge for the VSTLs.** In every certification test engagement, a manufacturer will challenge a VSTL's identification of a discrepancy based on interpretation of a standard. This is currently being handled through the EAC's request for interpretation (RFI) process. If a discrepancy cannot be tied to a very specific requirement in the VVSG, this can potentially create a contentious situation between the VSTL and the Manufacturer.

**NOTE:** To be clear, when SysTest Labs refers to testing in the context of the EAC's program and as defined by the VVSG and the EAC's certification test program, we include the definition for all reviews, assessments, demonstrations, and system executions, i.e., all "testing" activities defined in Part 3 of the VVSG.

4. How could the processes of the VVSG be modified to incorporate minor revisions without incurring the costs (time and money) of a total system test, and still maintain the integrity of the standard?

**Other industries have successfully managed both major and minor revisions to standards for many years and their models are available for review. The key is to establish a baseline of trusted certifications that can then be used as a stepping off point for future revisions to standards and thus future revisions to the manufacturer's voting systems. The challenge to date has NOT been that the standards have changed but that the process for testing and certification has changed and is in flux. The EAC has determined that previous NASED qualification testing efforts can not be used as a baseline for EAC certification and therefore, all voting system manufacturers that seek to associate their products with an EAC certification number must submit their systems to full EAC certification testing. The assumption is that once certified, subsequent enhancements to the systems and/or subsequent updates to the standards would only require certification testing of the changed components of the previously certified system (either for enhancements made by the manufacturer for customer needs or due to changes in the standards).**

5. What are the implications of the proposed usability benchmarks to you as a Voting System Test Laboratory? What are your current capabilities to test using human subjects?

We believe that the impact of the new usability benchmarks and associated Benchmark Test Methods on both a VSTL and a test campaign will result in requiring temporary test subjects and a modification of our test methods to include a significant “mock election” effort. The new usability requirements and test methods require that we gather a significant amount of data related to the voter experience, and by voter experience, this means test subjects as “actual voters” and not test engineers. The “actual voters” would include both disabled and non-disabled voters, where the disabled voters would include individuals with differing disabilities. In addition to the “actual voters” being engaged in the “mock elections”, SysTest Labs’ test engineers would be monitoring and recording all actions and events (as they would during all test execution) to record appropriate metrics. Although the usability benchmark metrics can be gathered throughout the entire test campaign, many of the requirements for usability involve subjective responses from the “actual voters” and the calculated metrics could change depending upon subjective data. This could create a situation that places the VSTL in a position of having to defend its results based on opinion rather than factual test results and put the VSTL in a contentious position with either the Manufacturer or the EAC.

SysTest Labs is fully capable of fielding a team of highly skilled and experienced human factors test engineers (full time employees) along with a sufficient number and variety of “actual voters” for the required duration of usability testing. We have used individuals from the Colorado Center for the Blind (CCB) for accessibility testing to ADA, HAVA, and Section 508 standards and have used and will be able to continue to use individuals with other disabilities, e.g., paraplegic and quadriplegic individuals. Obtaining a sufficient number of other non-disabled “actual voter” would be fulfilled through our association with Metropolitan State College, the University of Colorado at Denver, and the Community College of Denver all of which have both traditional (18 to 24) and non-traditional (24 and up) students.

6. Are there any changes to the VVSG, in either scope or depth, which would significantly reduce the cost (time and/or expense) of compliance without adversely affecting the integrity of the VVSG or the systems that are derived from its implementation?

We are preparing a relatively detailed set of feedback to the TGDC on questions regarding the VVSG. Included in this feedback are a number of changes that we feel could lead to greater efficiencies while maintaining the integrity of the VVSG. For example, treating certain activities within the certification testing campaign as an independent verification and validation activity, as discussed in the answer to question 3, could provide the level of in-depth review and assessment required to assure conformity without having to duplicate testing that has been completed either by the manufacturer or by accredited hardware testing labs. Earlier involvement by the VSTL during a Manufacturer’s SDLC could eliminate discrepancies that might not otherwise have been found until late in the certification test campaign and thereby creating significant delays.