THE ENGINEER'S GUIDE TO
WORLDWIDE REGULATORY
COMPLIANCE
www.conformity.com
Volume 13, Issue 10
October 2008

Conformity®

The IEEE Product Safety Engineering Society: *The First Five Years*

Emerging Issues in Standards

Improving Election Security and Accuracy: The Future of Voting System Certification

Challenges in Testing

Conformity Assessment and Accreditation: Their Role in the Global Market

Design Fundamentals

Design Issues in Extreme EMC Environments

Focus On...

Test Equipment

Conformity Magazine
531 King Street, Suite 6
Littleton, MA   01460
CHANGE SERVICE REQUESTED

by Stephen Berger, TEM Consulting

© Lisa F. Young | Dreamstime.com

Improving Election Security and Accuracy: *The Future of Voting System Certification*

A lot has changed in voting system certification since the 2000 presidential election. Those changes have now come to the place where more of the same will start doing more harm than good. Fundamental and needed changes in how voting systems are tested, certified and safeguarded have been made in the past 8 years. However, further improvements in total election accuracy, security, reliability and usability will require new approaches.

The changes that have been made are now having their effect on the certification process. Much can be learned by reviewing the current state of the system. Where the desired effect is being delivered, there are usually ways to refine the process and further enhance the outcomes. Where there are unintended consequences, modifications and adjustments are needed to avoid those negative and unintended consequences coming from needed changes.

Few systems improve by linearly extending what has been done in the past indefinitely. As the first round of changes made in response to the 2000 presidential election are making their impact, further improvements are seldom obtained by simply "doing more of the same." A next generation of improvements will come from innovations in new directions.

Part 1 of this article, which was published in the June issue of *Conformity*, looked at the changes that have been made, and where the U.S. system for certifying voting systems stands today. It analyzed the benefits that have been brought, but also the negative unintended consequences that could occur by simply doing more of the same.

To gain further improvements in elections, new approaches are needed to retain the benefits gained so far and to take the system to the next level of accuracy and security. So Part 2 of this article will explore the most promising new approaches that could further extend the benefits achieved so far.

Mutually Supportive Processes

One clear area for improvement is to analyze the different processes which currently operate largely in isolation, and coordinate them more effectively. Currently too many principle players operate in relative isolation. There is potential for significant benefit through enhanced coordination, so as to align efforts from different processes to be mutually supportive and increase the value they make to each other.

A principle cooperation exists between the National Voluntary Laboratory Accreditation Program (NVLAP) under the National Institute of Standards and Technology (NIST), and the Election Assistance Commission's (EAC's) Certification Program. NVLAP has the responsibility to assess and recommend laboratories to the EAC for accreditation. It then is responsible to monitor those laboratories' ongoing compliance with ISO Guide 17025, *General requirements for the competence of testing and calibration laboratories*.

In a nutshell, NVLAP is responsible for assuring that voting system test laboratories (VSTLs) have the ability to do a good job. The EAC on the other hand is responsible for reviewing the test plans, test reports and recommendations for system certification coming from the laboratories. The EAC decides whether to certify a voting system, and it relies on the testing at the VSTLs to make that determination. The EAC must examine the work product of the VSTLs and decide if it is up to expectations. Clearly, there is a lot to be gained by assuring that the assessment of a VSTLs ability to do good work, and the ultimate quality of the work it does produce is tightly coupled and using a common set of quality metrics.

Figure 1 illustrates the documentation each lab develops as part of its original accreditation. ISO Guide 17025 can be divided into two major sections. Laboratories are required to have test methods, adequately trained personnel, and the appropriate equipment to perform all testing within their scope of accreditation. Then, each lab is responsible for having documented laboratory management and quality processes to assure the ongoing consistency and quality of their work.

Figure 2 illustrates how this body of documentation is applied to every individual voting system to be evaluated. Specific test cases must be developed that properly apply the general test methods, and taken together, assure the complete and thorough evaluation of the voting system.

The EAC requires that VSTLs develop an individual test plan for every voting system evaluated. In the test plan the VSTL will analyze a specific voting system and create system specific test cases, using the test methods and standard lab procedures developed as part of their NVLAP accreditation. The plan produces a set of specific test cases for each system and explains how the set of test cases, together provide a complete and effective evaluation of the specific system to the requirements of the VSS/VVSG.

Another critical cooperation is between the EAC's Certification Program and state certifications. In general, states have only the most general understanding of what is done at the national level. The result is that state testing is often either redundant or alternately misses the same areas missed in the national program.

Ideally, the national program should test a core set of specifications common to most states. This saves the individual states from dealing with these issues. State certification can then focus on the specific issues and practices of that individual state. National certification intends to demonstrate the overall capability of a voting system. State certification should seek to identify systems that meet the specific needs of each individual state. There is overlap in these concerns, but there is also a great deal of difference.

At this writing, Brian Hancock, the inaugural director of the EAC's certification program, will be scheduling a meeting in the near future with state certification officials and others. The purpose of the meeting will be to explore ways that closer cooperation can be realized. Potentially one or more pilot efforts will be inaugurated from this collaboration.

The ultimate goal of all these efforts is to assure well run, accurate and secure elections. The top priority is that local election officials be able to use the voting system to run good elections, and to create records that prove that they ran a good election. The national and state certification programs could do more, through closer coordination of their efforts, to assure that local officials have the tools they need, and that those tools have been tested and proven to be reliable and effective.

It should be noted that, in these efforts by the EAC and state election officials, further improvements are being explored through improved process coordination. The first generation changes focused on launching the EAC (the new federal agency), developing new standards and a new lab accreditation program. Those were needed improvements. In these efforts, the EAC is seeking to bring further improvement

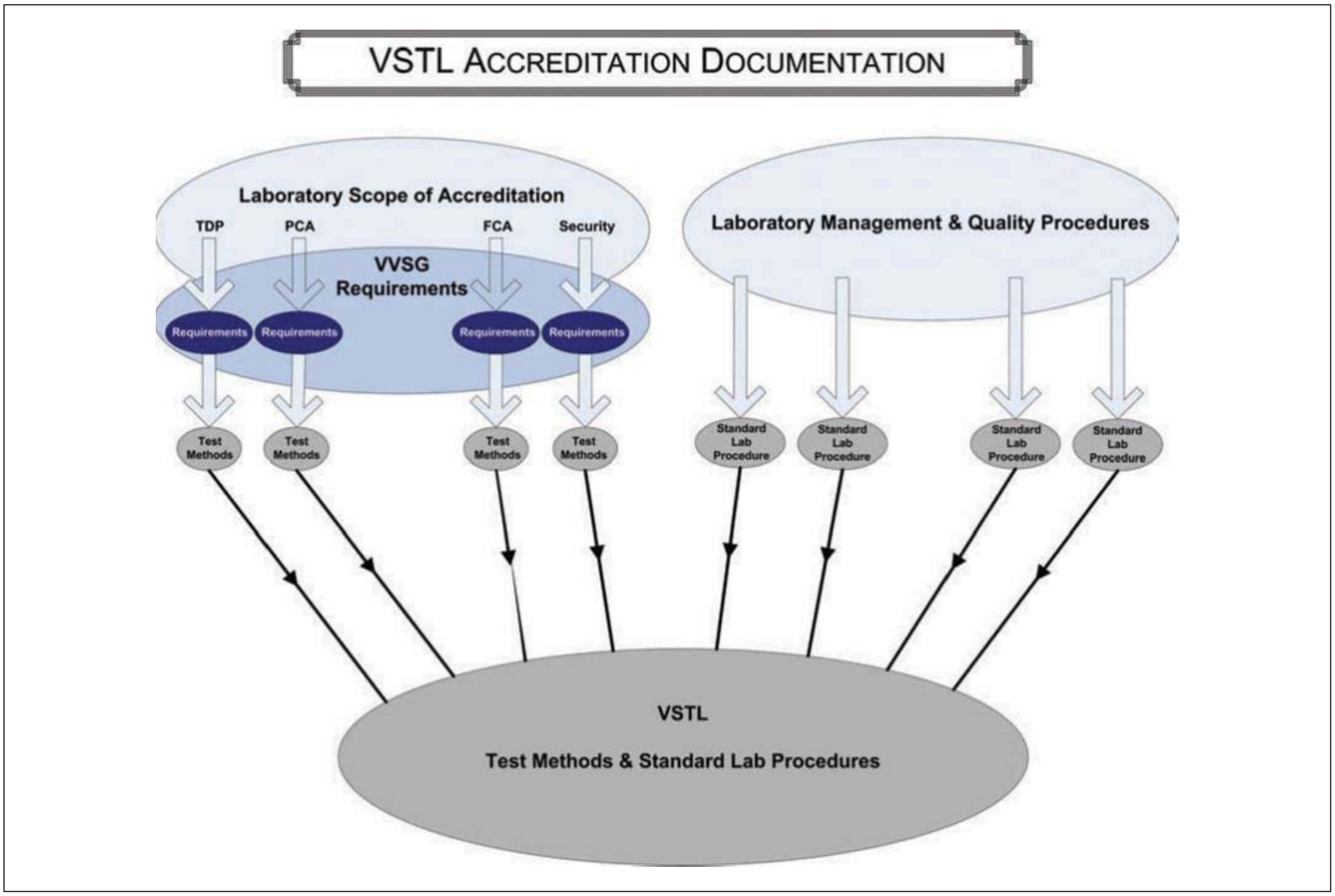


Figure 1: Using ISO Guide 17025, NVLAP assures that voting system test laboratories (VSTLs) have management processes, quality systems, and general test methods to evaluate voting systems.

by working on a different level, the level of coordinated processes.

Total System Improvement

The election system has received almost no system design or operational engineering, and opportunities for total system improvement abound. However, the diverse and distributed nature of the system makes coordinating such efforts particularly difficult.

A central issue facing elections is analyzing what it is ultimately dependent upon. Paper ballots relied on the ability of people to accurately count them. For security, election administration procedures were relied upon to assure that the ballots cast were accurately counted and included in the vote tallies. Unfortunately, the system of people, paper and procedures had a high rate of inaccuracy, human error and were susceptible to malicious tampering and fraud.

To reduce human error, automation was introduced. Voting machines dramatically improved the situation by replacing counts by people with machine counting. Security was improved by creating multiple separate electronic records of each vote. Multiple records makes it much harder to commit fraud because, to be successful, all copies must be changed. However, computerized voting systems have their own problems and vulnerabilities.

In general, the debate has been framed (largely by the popular media) as a choice between people and paper or computer systems. This is a false dichotomy, and one that has drawn attention and resources away from a much more important exploration. The more productive question is "What is the best combination of people, procedures and electronic system to achieve the best total result?"

What is starting to emerge is a "4–vote" system. Increasingly, the following elements provide checks and balances to assure secure and accurate elections:

- People following election administration procedures;
- Computer-based voting systems;
- Historical trends and polls;
- Independent system audit and computer forensic evidence.

The coordination of people and voting systems following well-develop election administration procedures is relatively solid. It is the last two elements that are less understood, especially the growing role of computer forensic techniques in elections.

An enormous and sophisticated body of expertise has been developed to help candidates running for office. Historical voting trends are maintained, often down to the individual precinct level. Polls help candidates judge how well their campaign efforts are fairing. We are all familiar with exit polls and other mechanisms for monitoring voters' opinions. What is often unrecognized is the roll this plays in election security. When election results come in that are out of line

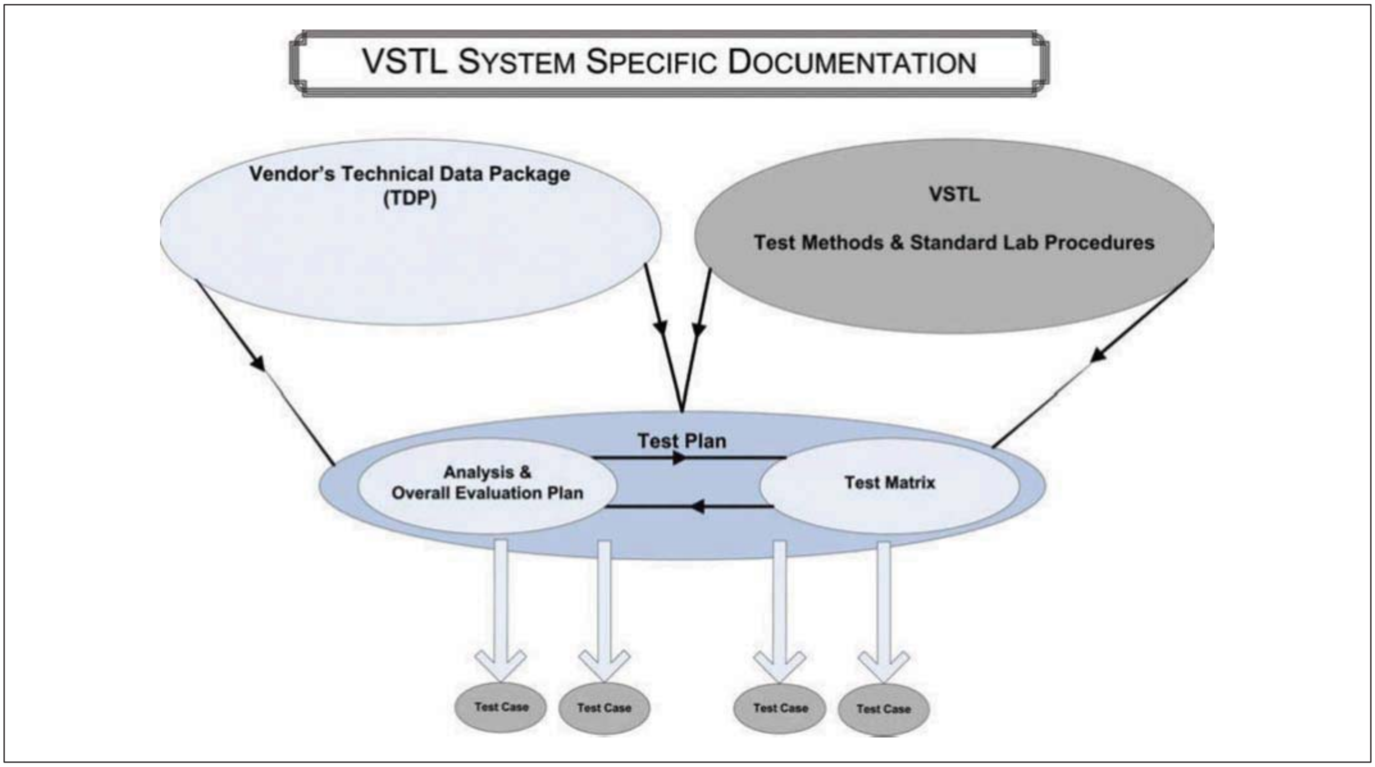

VSTL System Specific Documentation
Vendor's Technical Data Package (TDP)
VSTL
Test Methods & Standard Lab Procedures
Test Plan
Analysis & Overall Evaluation Plan
Test Matrix
Test Case
Test Case
Test Case
Test Case

Figure 2: The Election Assistance Commission is responsible for supervising how the VSTLs apply the general test methods to specific voting systems, and for the quality and accuracy of the evaluations they perform.

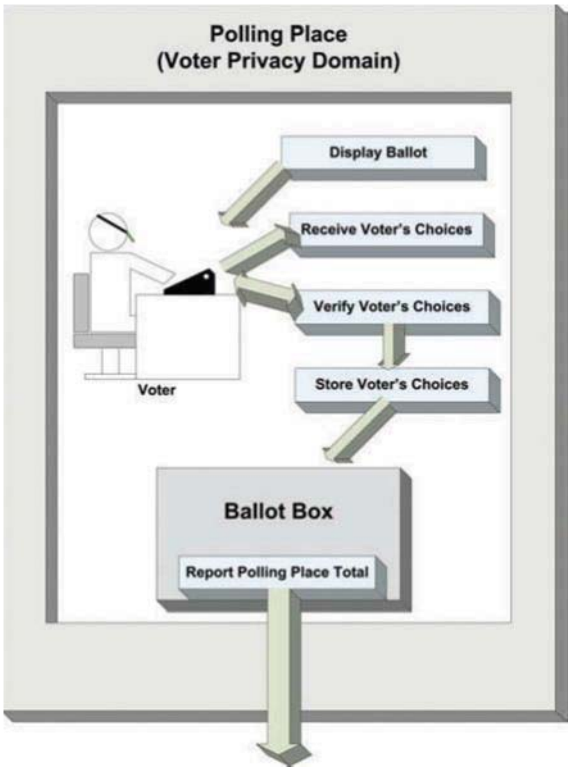


Figure 3: Voter Privacy Domain

with historical trends, polls or the expectations of a candidate, calls for an investigation are common. As a trigger for an investigation, this body of information forms a pretty good safeguard. After all, it would be pretty hard to rig an election without the vote totals looking odd, and triggering a call for an investigation from the losing candidate. Although far from perfect, it is an important safeguard.

The increasing use of computer forensic techniques is creating even more interesting benefits. An array of techniques are available, and state and local officials are starting to employ them.

One growing trend is the use of digital file signatures, commonly called HASH codes, to assure that voting system software has not been modified or tampered with. The Georgia Election Center at Kennesaw State has created a self-booting CD for the state of Georgia. When a system is booted from the CD, every file used by the voting system, including those files the voting applications use in the operating system, is examined and its digital signature is compared to the certified version of the software. The check takes 1.5 to 2 minutes and gives a GO/NO GO result. The check can be made before, after, and even during an election.

Parallel monitor testing is another growing tool being used. In a parallel monitor test, sample voting devices are pulled out of service and brought to a test location. The machines are then voted by people using scripts. Typically cameras record every keystroke made during the test. At the end of the election day, the totals are compared to what is expected from the scripts that were voted. The machines don't know that they are part of a test. If there is any malicious or malfunctioning software, the monitored test will reveal a difference in the total, leading to an investigation of the source of the discrepancy, and how widespread it is in the machines used in the actual election.

Other forensic tools are available but have not yet been applied in elections. One technique that security experts use in other areas is to run a separate monitor program simultaneously with an application. The monitor program, as an example, can monitor all reads and writes to election data files. Because all voting software is source code reviewed as part of national certification, the routines that will legitimately read or write election data are well known. The software that legitimately does this is both source code reviewed and extensively tested to assure it is secure and accurate. A monitor program could then simply confirm that only the expected software read and wrote to the election data files. If any other software accessed these files, a record and trigger for an investigation would be created. If the monitor program is provided by an organization separate from the voting software vendor, they become independent actors.

Situation Specific Security

The security requirements developed so far have taken something of a "one-size-fits-all" approach, and have failed to recognize that, in voting systems, there are two very different situations. The first situation is when the voter's identity can be linked to the ballot. A second situation exists once the ballot is anonymous and cannot be linked to the voter.

When a voter is voting, a lot of protections cannot be employed out of a need to protect voter privacy. Max Etschmaier, in a paper prepared for NIST, called this the "Voter Privacy Domain" (see Note 1). Figure 3 illustrates where privacy must be maintained, but also the limited functionality required within that domain.

Once the ballot is in the ballot box and separated from the identity of the voter, a different situation exists. At the point the ballot is separated from the identity of the voter, all the audit and tracking tools that are used in banking and for electronic commerce can be used. A ballot can be uniquely identified and tracked all the way to the final total. There is no reason not to have a traceable link between every ballot in the final total all the way back to the ballot box. Techniques exist and are well developed that would assure every ballot is included in the final total, and, equally, that no ballots from unknown locations have been added. There is no reason not to have this kind of solid audit data to link ballots from the ballot box to the final total.

North Carolina Director of Elections, Gary Bartlett, and Keith Long, that state's Voting Systems Director, have introduced an innovative new reporting system for the 2008 primary elections that illustrates both new innovations and this fundamental difference that takes place in the election process. In the North Carolina system, election results are reported through the North Carolina State Board of Elections website. Voters are able to monitor results as they are reported to the state, and the results in the total can be traced back to individual precincts.

A very different situation exists when the voter is in the voting booth and the ballot and voter's identify can be connected. In this situation, a lot of security measures cannot be used because they would violate the privacy of the voter. However, the voting situation is much simpler than that facing the total voting system. In the voting booth, the following actions must be accomplished:

- The ballot must be presented to the voter;
- The voter's choices must be recorded;
- The voter must be given a chance to confirm the ballot choices and cast the ballot.

Considering the relative simplicity of the task, a number of measures can be conceived that would secure this situation. One of the interesting features of voting systems is the relative lack of using write-once media. There is little reason for not having one piece of software present the ballot to the voter and record the voter's choices on a write-once CD or other media. A second software package, potentially provided by a trusted 3rd party, could then read the recorded ballot and have the voter confirm the choice. If the voter confirms the ballot, the second software would sign the ballot on the media. If the voter chooses to recast the vote the process would be restarted and the validation software would spoil the ballot instead of signing it. Such a system essentially puts two independent witnesses into the voting booth, and creates an indelible record of the ballot.

Crafting security requirements that are situation sensitive would greatly increase the total security of the election system. Today, powerful security practices are being denied the election system because they would violate voter privacy. There is no reason to deny these practices to the entire system. They only need to be denied in the voter privacy domain, where the voter's identity and ballot can be linked. Conversely, other techniques are currently not used in the voter privacy domain because they would be too complex to use in the entire voting system. However, the situation when the voter is in the voting booth is a much simpler situation. A great deal can be done to protect the voting booth situation that would be impractical to do in the entire voting system.

Model Driven Architecture

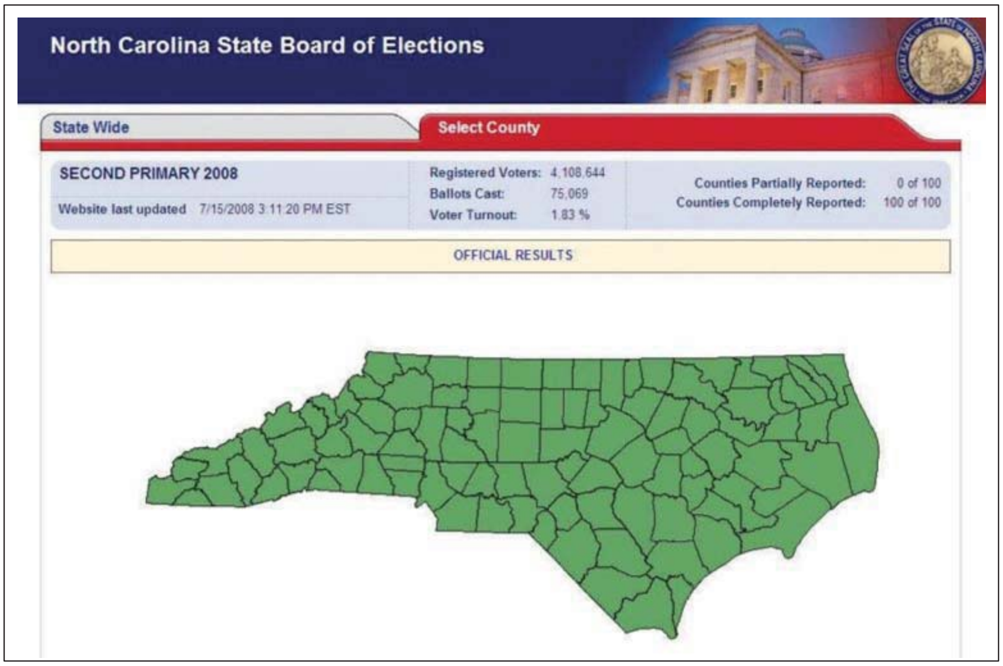
One of the primary problems facing those trying to improve voting system certification is that, while voting systems are enormously important as a business, it is a small, niche

industry. Only about six companies have sold any significant amount of equipment. Total sales amount to a few hundred thousand units per year. Therefore, the resources available to design and implement changes are very limited.

A second challenge is the tremendous amount of detail that must be addressed. The current voting system standard has about 1000 separate requirements. Each of these must be tested, and each system requires different tests due to the vendor's unique design.

What is needed is a way to treat systems from different vendors in a similar way, sharing cost for things like development of test automation. Also needed are ways to group many details by abstracting up to a higher level and treating many details together. Perhaps the most promising way to do this is through a model-driven architecture (MDA).

An MDA is a way of describing a system using a platform, technology and vendor-independent model. The Object Management Group (OMG, see Note 2) has refined and structured the process by developing a unified modeling language (UML) to support formal model-driven architectures (MDA).


North Carolina State Board of Elections

State Wide | Select County

SECOND PRIMARY 2008

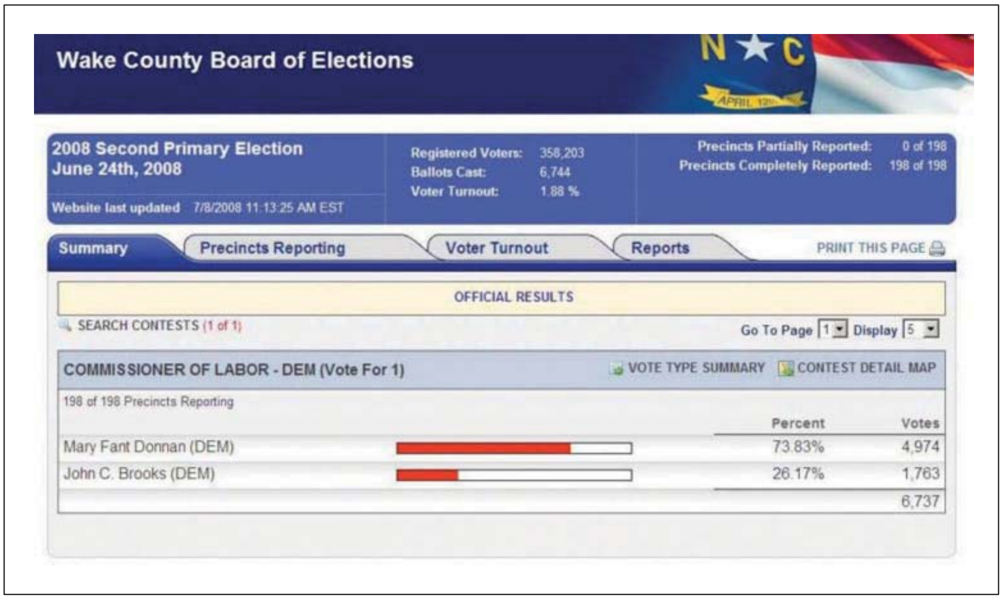
Website last updated 7/15/2008 3:11:20 PM EST

Registered Voters: 4,108,644
Ballots Cast: 75,069
Voter Turnout: 1.83 %

Counties Partially Reported: 0 of 100
Counties Completely Reported: 100 of 100

OFFICIAL RESULTS

Figure 4: North Carolina's innovated election reporting service


Wake County Board of Elections

2008 Second Primary Election
June 24th, 2008

Website last updated 7/8/2008 11:13:25 AM EST

Registered Voters: 358,203
Ballots Cast: 6,744
Voter Turnout: 1.88 %

Precincts Partially Reported: 0 of 198
Precincts Completely Reported: 198 of 198

Summary | Precincts Reporting | Voter Turnout | Reports | PRINT THIS PAGE

OFFICIAL RESULTS

SEARCH CONTESTS (1 of 1)

Go To Page 1 Display 5

COMMISSIONER OF LABOR - DEM (Vote For 1)

VOTE TYPE SUMMARY | CONTEST DETAIL MAP

198 of 198 Precincts Reporting

	Percent	Votes
Mary Fant Donnan (DEM)	73.83%	4,974
John C. Brooks (DEM)	26.17%	1,763
		6,737

Figure 5: North Carolina's system provide reports down to the individual precinct, allowing analysis of voting trends and tracking of votes back to the precincts.

A complete MDA specification has three levels, a computer-independent model (CIM), a platform-independent model (PIM) and a platform-specific model (PSM). UML is used to provide a tight connection between the CIM, PIM and PSM models, assuring that each is an accurate implementation of the other. A well-developed MDA consists of a computer and platform-independent base UML model, with one or more platform-specific models and interface definition sets. Each set describing how the base model is implemented on different platforms, using different technologies from different vendors.

For elections, an MDA would provide a way to plan and coordinate election administration, voting systems, audit and forensics and the certification process. The MDA focuses primarily on the functionality and behavior, not the technology. It separates implementation details from functions, but defines interface points to assure effective communication. This allows all systems to be planned and analyzed, and high-level, universal requirements to be developed. The lower level models bring forth implementation nuances and require decisions on how high-level requirements will be realized using specific platforms and architectures. With MDA, functionality and behavior are modeled once and only once.

There are some very logical divisions that, if defined under an MDA, could release powerful new capabilities for elections and voting systems. Both OASIS and the IEEE have worked on standards defining electronic data interchange formats for voting system. These efforts contain within them the common data exchange points in all voting systems, and define common formats for those data records.

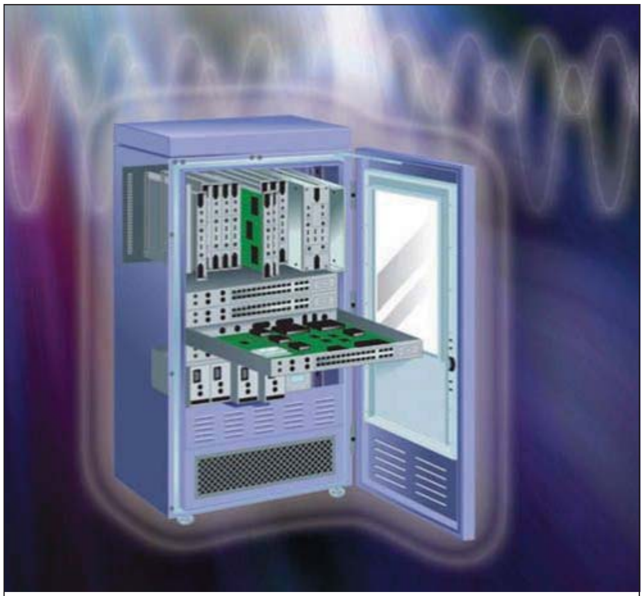
The uniqueness of the voting booth situation has been discussed. If, under an MDA, standard and vendor-independent file formats were specified for both ballots and cast vote records, and the interface from the voter's interface were standardized, a number of possibilities would be created. For example, during certification testing, voting machines could be presented with hundreds, even millions, of ballots, and simulated votes could be cast with the resulting cast vote records checked for accuracy.

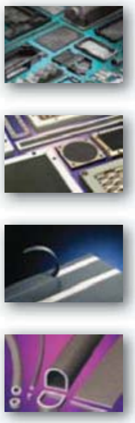
Currently, this type of testing is performed by hand, and only a small number of ballots and votes are used in testing a system. This testing can miss infrequent errors or errors that only result when large numbers of votes or certain patterns of votes are cast. Being able to create vendor-independent, automated tests would allow much more thorough testing. Further, if the test tools are vendor-independent, then the evaluation of vendor systems would be more equitable because they would all be subjected to the same testing.

Another possibility created would be to have software provided by independent companies performing different functions and cross checking each other. For example, software from one company could present the ballot to the voter and record the voter's choices. Software from a different company could then present the choices on the cast vote record to the voter for verification. Using encrypted signatures each piece of software could separately sign the cast vote record and only votes with two valid signatures would be accepted. Even different hardware could be used, making such systems both software and hardware isolated.

Auditing and Forensics

Perhaps the most promising area for bringing further improvement in the election system is in the area of auditing and forensics. MDA opens the possibility of designing a independent but systematic auditing and forensic system. If key points in voting systems were defined and standardized across all systems, then audit and computer monitor systems could be designed to record elections activity independently of the vendor-provided hardware and software.



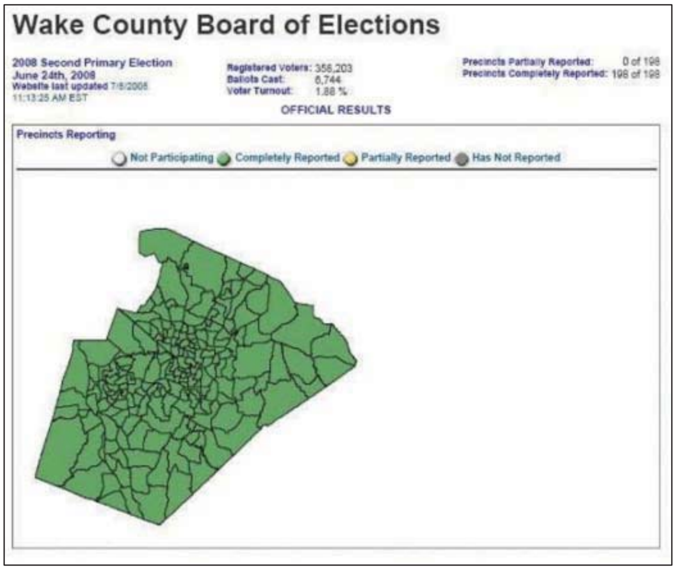


A robust audit system essentially becomes a third component in the election process. There would be:

- People and administrative procedures
- Voting systems
- Auditing systems

Designed thoughtfully, each provides protections for the vulnerabilities of the other. For critical issues there should be redundant safeguards in the administrative procedures and in the voting system. If in any way both of those sets of safeguards fail, then the audit system should detect the failure and alert officials to it.

In contrast to the ineffective attempt to test quality by adding more and more specifications and tests to the voting systems, taking a system-design approach offers real promise. Integrating well-designed audit systems, provided independently of the voting system vendors, builds in new security and accuracy protections at far less total cost than most other improvements. Using each of these elements in a thoughtfully integrated system design offers real promise of substantial improvement. Such a defense-in-depth design stands in real contrast to a nostalgic but flawed return to people and paper, or a naïve reliance on computerized voting systems.



Wake County Board of Elections

2008 Second Primary Election
June 24th, 2008
Website last updated 7/5/2008
11:13:25 AM EST

Registered Voters: 356,203
Ballots Cast: 6,744
Voter Turnout: 1.88 %

Precincts Partially Reported: 0 of 198
Precincts Completely Reported: 198 of 198

OFFICIAL RESULTS

Precincts Reporting

○ Not Participating ● Completely Reported ● Partially Reported ● Has Not Reported

Figure 6: Precinct map of Wake Country, North Carolina

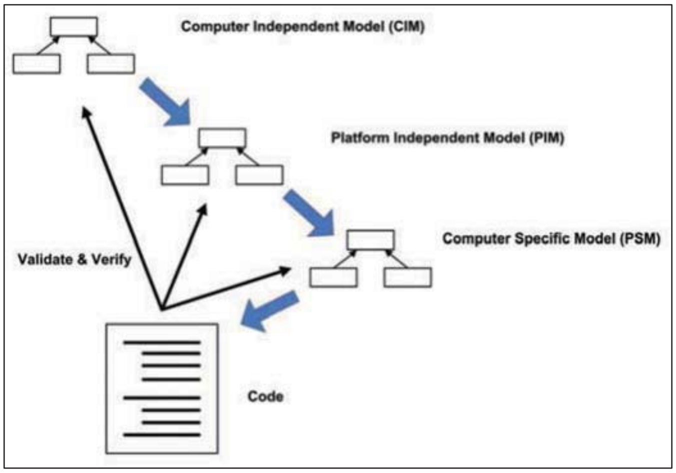

Computer Independent Model (CIM)
Platform Independent Model (PIM)
Computer Specific Model (PSM)
Validate & Verify
Code

Figure 7: Key concepts of model-driven architecture (MDA, see Note 3)

Conclusion

The United States election system has undergone revolutionary change since the 2000 presidential election. A new federal agency, the EAC has been created and taken leadership in certifying voting systems. A new system of voting system laboratory accreditation has been installed. Fundamental new protections have been introduced in all levels of the election system. The system on which voters will cast their ballots in 2008 is a far different system than the one they voted on eight years ago.

What has become manifestly clear is that there are unintended negative consequences to some past actions. The past failure to provide laboratory-verified test methods with the 2002 standard has allowed some equipment flaws to get into the field. The EAC is taking action to develop standardized and verified test methods, but those efforts have not yet been completed.

The cost of certification has gone up an order of magnitude since 2000 and appears destined to rise even higher. The challenge is to divine how to retain the improvements while at the same time avoiding the unintended consequences, such as the cost and time required for certification.

The opportunity that exists today is to build on the significant changes that have been made, not by doing more of the same, but by launching in new directions. The opportunity is present to develop a system architecture and integrate administrative procedures, equipment and an audit system to provide a system with profound accuracy, fault tolerance and security with defense-in-depth. □

Stephen Berger *is the principle of TEM Consulting, and can be reached at stephen.berger@ieee.org.*

Notes

1. Maximilian M. Etschmaier, "Voting Machines: Reliability Requirements, Metrics, and Certification," September 2006.
2. www.omg.org
3. Figure adopted from a presentation, "OMGs MDA and Software Radio," presented January 25, 2006 at the IEEE 1900 plenary meeting in Boulder, CO by Fred Waskiewicz, Director of Standards Object Management Group, wask@omg.org.

FAST Link www.conformity.com/2240