

# **Elections, Technology, and the Pursuit of Integrity: the Connecticut Landscape**

Theodore Bromley<sup>1</sup>

Peggy Reeves<sup>2</sup>

Alexander Shvartsman<sup>3</sup>

## **Abstract**

Transition from lever voting machines to electronic voting technology in Connecticut necessitated the development of new policies and procedures by the Secretary of the State (SOTS) Office to safeguard the integrity and security of the new electoral process. Forming a partnership with the University of Connecticut, SOTS Office developed a comprehensive approach that extended the existing electoral procedures to incorporate the use of the new optical scan electronic voting equipment. This paper reports on the overall electoral process in Connecticut that includes new procedures that ensure strict chain-of-custody control of the electronic voting machines, safe-use of the memory cards used to program the machines for each specific district and election, and the audits performed in conjunction with each state-wide election. The comprehensive audits in Connecticut consist of hand-counted audits in 10% of randomly selected districts, and technology audits that focus on pre-election and post-election audits of memory cards. The detailed audit reports are published upon their completion. In addition, technical inspections are performed of any voting machines that possibly may not have operated correctly. The partnership between the SOTS Office and the University of Connecticut is one of the most unique examples of collaboration between state government and academe in ensuring the technological integrity of the electoral processes.

---

<sup>1</sup> Office of the Secretary of the State, State of Connecticut, 30 Trinity Street, Hartford, CT 06106

<sup>2</sup> Office of the Secretary of the State, State of Connecticut, 30 Trinity Street, Hartford, CT 06106

<sup>3</sup> Center for Voting Technology Research, Unit 2155, University of Connecticut, Storrs, CT 06268

## **1. Introduction**

The Secretary of the State of Connecticut (SOTS) is statutorily defined as the Commissioner of Elections for the State.<sup>4</sup> As such, the office is charged with the administration of all elections held within the State. The goal of the office is to ensure that all elections are conducted in a fair and impartial manner and that the citizens of the state have faith in the integrity of the process. When the State of Connecticut moved from lever voting machines to electronic voting equipment many of the processes regarding the administration of elections changed. The introduction of new voting technology made it necessary to ensure that the new procedures and safeguards were adhered to in all respects. To this end, an audit process was developed for use with this new technology. The process includes a hand-counting component and a technological component. To facilitate the development of the technological audits, the office formed a partnership with the University of Connecticut Center for Voting Technology Research (VoTeR Center), whose mission is to advise state agencies in the use of voting technologies by investigating voting solutions and equipment and developing safe use election procedures. Through this partnership the State of Connecticut has been able to continually investigate and improve upon its use of electronic voting equipment.

## **2. Overview of the Electoral Process**

The preparation of the new voting equipment starts after the State- defined endorsement period for all candidates who will appear on the ballot. Once the election information that will appear on the ballot is finalized, the technical preparation for the elections commences. The ballot information is used to program the memory cards for each district participating in the election. Upon receiving the programmed memory cards, the local officials perform a series of logic and accuracy tests on the voting equipment. The most critical part of the logic and accuracy (L&A) tests of the optical scan (OS) voting equipment is to ensure that (1) the memory card is programmed appropriately for the specific election and district, (2) the tabulator is correctly reading and tallying the ballots fed through the scanner, and (3) no technical failures have occurred prior to or while performing the L&A tests. We now present the overall process in more detail.

---

<sup>4</sup> Conn. Gen. Stat. Sec. 9-3

*Prior to Election Day.* Programming of the memory cards is carried out for the OS machines of each precinct by an independent vendor. The candidate information and ballot placement is sent to the vendor who programs each memory card independently and specifically for the unique ballot of the polling location. In addition, the machines undergo routine maintenance and testing to ensure the machine is properly functioning (according to the vendor-provided test procedures) independent of the memory cards. Once the memory cards are ready, they are securely transported to the polling locations and installed into the OS machines by the local election officials who conduct the prescribed pre-election logic and accuracy tests. This includes the development of test ballots that are marked with pre-determined marks and results. The ballots are then processed by the OS machine and the results are tabulated to ensure they match the pre-determined results. Once the OS performs in the manner anticipated, the machines are sealed and locked until Election Day.<sup>5</sup>

*On Election Day.* Before the polls open, the election officials verify seals on each OS machine, ensure they are undisturbed, set the machine(s) to “election mode,” and verify that the machines are properly initialized and that all election counters are set to zero. After the polls open, each voter is entitled to cast a single ballot once such voter is verified against the voter registration database. After the voter completes the ballot, the voter feeds the ballot into the OS machine.

*After the polls close.* Once the polls close and all voters have cast their ballots, the election officials at the polls print the vote totals report directly from the OS machine. Connecticut uses a manual tabulation method of the votes using these vote totals reports from each district. The reports from each separate polling location are delivered to the central tabulation location where the totals from the various polling location reports are combined, computed and reported to the Secretary of the State for certification. (We note that one of the reasons for using this manual tabulation method is to avoid the technological risks associated with the use of computer-assisted central tabulation).

*Hand Count Audit* occurs after the election is over and after the state mandated lock-down period for the voting equipment. In Section 3 we describe the hand count audit in more detail.

---

<sup>5</sup> Conn Agencies Regs. Sec. 9-242a-5 (2008)

*Technological Audits.* In addition to hand count audits, in each state-wide election, technological audits are performed. The technological audits include the following three components (a) the *vendor audit* that focuses on the integrity and security of the electronic election systems, (b) the *pre-election audit* that focuses on the correctness and integrity of the programming of the electronic equipment before the election, and (c) the *post-election audit* that determines whether the electronic equipment functioned and was used in a way that is consistent with the proper conduct of the election. The pre- and post-election audits are described in more detail in Section 4.

The overall electoral process is depicted below in Figure 1.

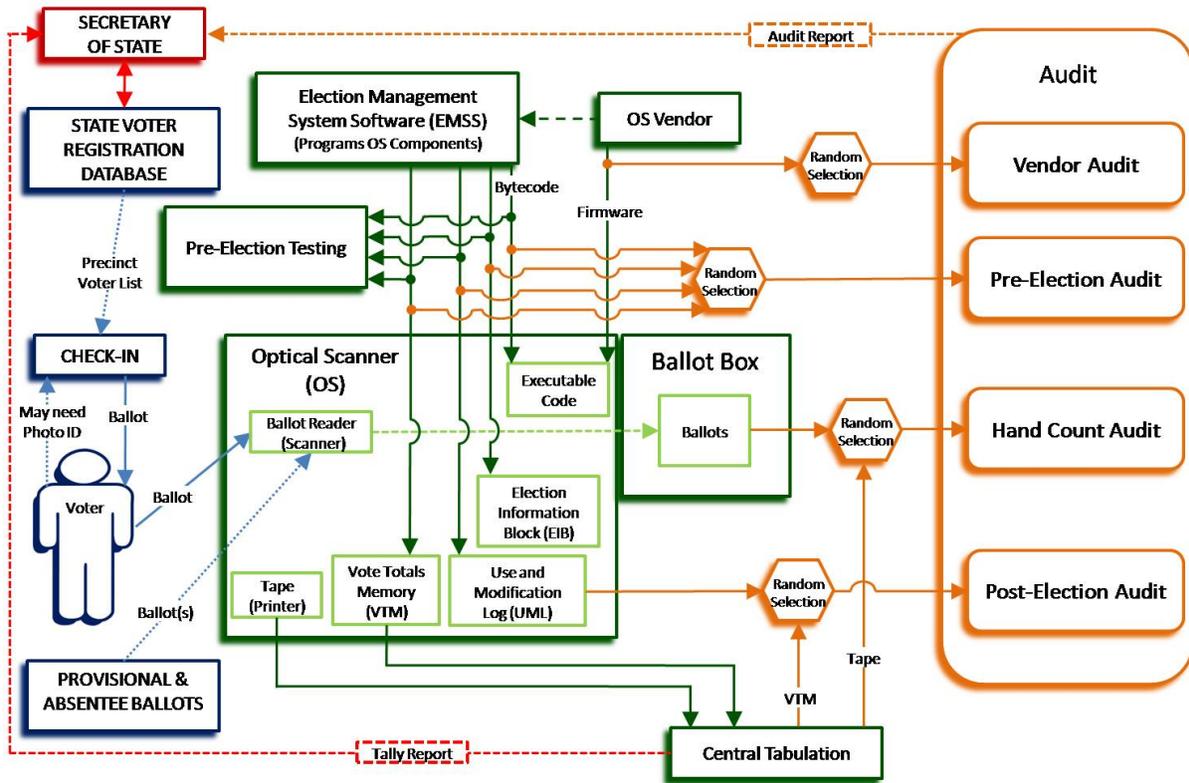


Figure 1. Election Process Diagram for Optical Scan Election Systems.

The processes in the left part of the diagram (the red Secretary of State role, the blue components involving the voters, and the green components dealing with the use of optical scan technology) are typical, and common to most states that use optical scan tabulation. By contrast, the orange

components on the right side of the diagram depict a comprehensive approach to audits – both hand counted and technological – are largely unique to Connecticut.

### **3. Hand Count Audit**

The hand count audit requires an actual hand count of the ballots processed by the OS tabulators and a comparison of the hand counted results to the results provided by the OS tabulators.<sup>[6]</sup> This process after the election can detect any discrepancies between the machine counts and the actual votes cast. The audit helps ascertain the accuracy of the scanning device and the reliability of the counting process.

Mandatory post-election hand count audits are conducted by local officials in ten percent (10%) of the voting districts randomly selected to participate. The primary purpose of the hand count audit is to assess how well the optical scan voting machines functioned in an actual election and to ensure that votes cast using these machines are counted properly and accurately. Once the voting districts subject to audit are identified, each municipality sets its audit date individually. It is important to note that this procedure is not a complete recount of the election; there are separate statutory requirements for a mandated recount. The hand count audit includes only those ballots that were counted by the optical scan voting machine in the district that will be included in the audit and only in randomly- selected races. Critical in the assessment of the OS is to ensure that the hand count audit compares appropriate ballots and candidate totals to those reported by the OS. As such, certain specific requirements are necessary to ensure this comparison. First, the total number of paper ballots read by each optical scan machine should be recorded and used as a check to assure that all ballots counted by the machine are included in the audit. Second, ballots are categorized and assigned to one of the following two categories: “*Undisputed Ballots*” and “*Ballots with Questionable Votes.*” Undisputed ballots are ballots that should have been read by the optical scan voting machine. In other words, a review of the ballot in question reveals that each oval is completely filled in; there are no apparent problems, voter errors, unusual markings or noticeable stray marks in or around any of the races to be audited.

---

<sup>6</sup> For the definition of the audit see Connecticut Public Act 07-194 AN ACT CONCERNING THE INTEGRITY AND SECURITY OF THE VOTING PROCESS, approved July 5, 2007.

“*Ballots with Questionable Votes*” are ballots that contain problems, such as voter errors (e.g., check marks in the candidate’s oval), or stray or unusual markings in any of the races being audited. Such problems, errors or markings may have interfered with the optical scan machine’s count.

Once the ballots are separated, the audit workers shall count the votes for each candidate in each of the audited races on each ballot—first, from the Undisputed Ballots, i.e., ballots with no questionable markings; next, from the Ballots with Questionable Votes, i.e., where questionable markings appear for the particular race and candidate. The audit workers will keep separate vote totals for each candidate from both categories of ballots.

Once the hand count audit is complete, the results are reported to the Secretary of the State. Each “Questionable Vote” must be explained in the comments section of the audit report. If the machine total is different from the overall hand count total, then every effort must be made to investigate and explain why such is the case, including conducting a second hand count, if necessary. Any difference should be reported to the Secretary of the State. If the results of the hand count audit reveal any unexplained deviations or errors, The University of Connecticut (UConn VoTeR Center), at the request of the Secretary of the State, shall examine the machines that apparently produced incorrect results to determine if such errors were caused by the optical scan voting machine.

#### **4. Technological Aspects of Ensuring Election Process Integrity**

In addition to these procedures and testing, the University of Connecticut conducts additional testing and analysis to ensure the memory cards and tabulators perform correctly.

*Pre-deployment assessment of integrity and security.* Prior to deploying the optical scan voting systems in Connecticut, the Secretary of the State (SOTS) Office requested that the VoTeR Center perform an assessment of integrity and security of AV-OS tabulators. In particular the Center was asked to evaluate a report <sup>[7]</sup> that documented a security vulnerability of AV-OS, the so-called “Hursti Hack,” and investigate any other vulnerabilities of the system. The investigation by the Center

---

<sup>7</sup> Harri Hursti, Critical Security Issues with Diebold Optical Scan Design, Black Box Voting Project, July 4, 2005 (<http://www.blackboxvoting.org/BBVreport.pdf>).

established that the memory cards used with AV-OS can be tampered with, thus proving the seriousness of the Hursti Hack. The Center also discovered new security vulnerabilities of the AV-OS system.<sup>[8]</sup> We note that if the memory cards or the AV-OS tabulators are left unattended — within or without the tabulator — they can be tampered with in a matter of minutes. The effects of tampering with the AV-OS and memory cards on the election outcome can be devastating: votes cast on ballots can be reassigned to arbitrary candidates, leading to invalid election results. Subsequent reports by the Center document additional integrity issues with AV-OS systems.<sup>[9,10,11]</sup> In particular, it was determined that even if the memory card is sealed and pre-election testing is performed, one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and without having ever to access the card physically or opening the AV-OS system enclosure. For example, the attacks can lead to the following: neutralizing candidates (the votes cast for a candidate are not recorded); swapping candidates (the votes cast for two candidates are swapped); biased reporting (the votes are tabulated correctly, but they are reported incorrectly using conditionally-triggered biases).

Additionally, more severe threats become possible if the tabulator is left unattended and its internals are tampered with. Note that pre-election testing using vendor-provided methods may not be able to detect tampering (self-auditing is inadmissible, just as it is not admissible in the fiscal realm). The only way to guarantee that the memory cards contain valid data and programming for a particular election, is to directly examine the contents of the cards.

---

<sup>8</sup> VoTeR Center, Security Assessment of the Diebold Optical Scan Voting Terminal, October 30th, 2006 ([http://voter.engr.uconn.edu/voter/wp-content/uploads/uconn\\_report-os.pdf](http://voter.engr.uconn.edu/voter/wp-content/uploads/uconn_report-os.pdf)).

<sup>9</sup> A. Kiayias, L. Michel, A.C. Russell, N. Sashidar, A. See, and A.A. Shvartsman, An Authentication and Ballot Layout Attack Against an Optical Scan Voting Terminal, USENIX Electronic Voting Security Workshop (EVT07), Electronic proceedings (<http://voter.engr.uconn.edu/voter/wp-content/uploads/evt07.pdf>), August 2007

<sup>10</sup> A. Kiayias, L. Michel, A.C. Russell, N. Sashidar, A. See, A.A. Shvartsman, S. Davtyan. Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting. 23rd Annual Computer Security Applications Conference (ACSAC). Electronic proceedings. December 10-14, 2007 (<http://voter.engr.uconn.edu/voter/wp-content/uploads/seea-tamperevoting.pdf>).

<sup>11</sup> S. Davtyan, S. Kentros, A. Kiayias, L.D. Michel, N.C. Nicolaou, A. Russell, A. See, N. Shashidhar, A.A. Shvartsman: Taking total control of voting systems: firmware manipulations on an optical scan voting terminal. ACM Symposium on Applied Computing (SAC), pages 2049-2053, Honolulu, Hawaii, USA, March 9-12, 2009 (<http://voter.engr.uconn.edu/voter/wp-content/uploads/sac09.pdf>).

*Mitigation: addressing security and integrity in Connecticut.* As the result of these findings, the Center recommended to the SOTS Office that (a) strict chain-of-custody policies for AV-OS and memory cards need to be implemented, and (b) audits — both technological and hand-counting — need to be performed in conjunction with (at least) each state-wide election. These recommendations have been implemented in Connecticut starting with the November 2007 elections.

The SOTS Office asked the Center to prepare for and implement technological memory card audits for general elections that use AV-OS terminals in Connecticut. The Center developed a comprehensive methodology and associated tools for performing technological audits<sup>[12,13]</sup> and has performed technological audits in Connecticut in each state-wide election (and selected primaries) since 2007.<sup>[14]</sup>

The Center developed two types of technological audits:

1. Pre-election audit: This technological audit is performed on the memory cards randomly selected at districts for the audit after the pre-election testing conducted at the districts. Pre-election auditing includes integrity checks of the contents of the memory cards that are to be used in the elections, and the analysis of the audit log for adherence to proper election procedures and any unexpected events. This is achieved by contrasting the contents of the cards against a trusted database containing anticipated card contents. Any adversary that affects EMS (Election Management System) would be thwarted with the recognition of unexpected content. Attacks against the ballot layout geometry can also be detected. One must also account for “man in the middle” attacks that interfere with the data transfer between the EMSS and the removable media. Such attacks can also be detected by pre-election audits.

---

<sup>12</sup> T. Antonyan, S. Davtyan, S. Kentros, A. Kiayias, L. Michel, N. Nicolaou, A. Russell, and A.A. Shvartsman. Automating Voting Terminal Event Log Analysis. *Proceedings of the 2009 USENIX/ACCURATE Electronic Voting Workshop (EVT/WOTE 2009)*, 15 pages, electronic edition, Montreal, Canada, August, 2009 (url: <http://voter.engr.uconn.edu/voter/wp-content/uploads/evt09.pdf>).

<sup>13</sup> T. Antonyan, S. Davtyan, S. Kentros, A. Kiayias, L. Michel, N. Nikolaou, A. Russell, A. A. Shvartsman. State-wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity. *IEEE Transactions on Information Forensics & Security*, volume 4, issue 4, pp. 597-610, December, 2009 (url: <http://voter.engr.uconn.edu/voter/wp-content/uploads/ieee.pdf>).

<sup>14</sup> A.A. Shvartsman et al., Technological Audits of Optical Scan Voting Systems: Summary for 2007 to 2010 Connecticut Elections, Ver. 1.1, (<http://voter.engr.uconn.edu/voter/wp-content/uploads/VC-TechAudits-2007-2010c.pdf>), October 19, 2011.

2. Post-election audit: This technological audit is performed on the memory cards that were used in an election and submitted by the districts after the election. Similar to the pre-election auditing, post-election auditing includes integrity checks of the contents of the memory cards that are to be used in the elections, and the analysis of the audit log for adherence to proper election procedures and any unexpected events. The audit can detect irregularities in the voting process, e.g., if an adversary tampers with the media card during an election so that a biased output is produced.

The analysis performed during technological audits yields results that cover the following areas:

- Correctness of memory card programming (both data and code),
- Reliability of memory cards, and
- Adherence of the election officials and poll workers to proper procedures and sequencing of election activities, including: Pre-election testing, Preparation for elections, and Election Day procedures and processing.

Additionally, to enhance the integrity of the electoral process, the State implemented the following:

- i. explicit chain-of-custody procedures for the electronic voting machines and their removable media,<sup>[15]</sup> and
- ii. hand-count audits of 10% of the districts in each state-wide election as described earlier.<sup>[16]</sup>

We next describe the technological audits in more detail.

*Pre-Election Technological Audit.* These audits have three primary goals:

- i. determine whether or not the memory cards are properly programmed for the specific district and specific election,

---

<sup>15</sup> For example, see MODERATORS HANDBOOK FOR ELECTIONS AND PRIMARIES: OPTICAL SCAN VOTING TABULATORS, Office of the Connecticut Secretary of the State, revised October 2009.

<sup>16</sup> For the definition of the audit see Connecticut Public Act 07-194 AN ACT CONCERNING THE INTEGRITY AND SECURITY OF THE VOTING PROCESS, approved July 5, 2007.

- ii. determine whether or not proper pre-election procedures are followed by the election officials, and
- iii. determine whether or not any technical failures occurred.

Prior to the election, each polling center receives four programmed memory cards from the external contractor. According to the instructions from the SOTS Office, each district is supposed to perform pre-election tests of the four cards. After the testing is complete, they are asked to select randomly one memory card per district and send it to the Center for pre-election technological audit. The procedure for random selection of memory cards applies to district-based tabulators and does not include central absentee ballot tabulation. When the cards are submitted for the audit after they undergo pre-election testing and preparation for the election, such memory cards should be in “election mode” with all counters set to zero.

As the cards arrive from the districts at the Center, the contents of the cards is examined to determine whether the data and code on the cards is correct for the given district and election, and whether the pre-election testing was performed and the cards are set for election. This is done by comparing the card contents to the known baseline data received from the external contractor, and by checking the status of the card and its audit log, which should contain the time-stamped events that correspond to the cards being programmed, tested, and set for election.

*Post-Election Technological Audit.* Post-election audits deal with the memory cards that were used in the election, and have three primary goals:

- i. determine whether or not the memory cards are still properly programmed after the election is closed for the specific district and specific election,
- ii. determine whether or not proper pre-election procedures are followed by the election officials, and whether the usage of the cards is consistent with the proper conduct of the election, and
- iii. determine whether or not any technical failures occurred. The post-election audit employs a procedure similar to the pre-election audit.

The selection of cards for the post-election technological audit differs from the pre-election audit as follows. The SOTS Office randomly selects 10% of the districts that are the subject of post-election hand-counted audit. These districts are also asked to submit the cards that were used in the election for the post-election technological audit. Additionally, any district, in principle, is able (and welcome) to submit their cards for the post-election audit.

As the cards arrive from the districts at the Center, the contents of the cards are examined to determine whether the data and code on the cards are correct for the given district and election, and whether the events recorded in the card's audit log correspond to a proper programming, preparation for the election, and conduct of the election. This is done by comparing the card contents to the known baseline, and by checking the status of the card and its audit log.

The technological audits in Connecticut have been performed in conjunction with each state-wide election since 2007. For additional information we refer the reader to the collection of the audit reports available online.<sup>[17]</sup>

Finally, we note that our technological audits provided the first statistical documentation of the reliability of memory cards used with the AV-OS the electronic components used in the elections. In particular, we estimated the overall percentage of the cards that are not usable in the election to be between 7.4% and 17.4%. None of these cards are readable by the tabulators, and as such they do not pose a security concern: such cards are detected as unformatted cards by the tabulators and they cannot be used in the election. However, this high failure rate is a reliability issue. Our earlier investigation determined that the primary reason for memory card failures is depleted batteries.<sup>[18]</sup> Once the battery's store of energy is depleted, the cards lose their data. The electrical properties of the batteries are such that the battery voltage output can decrease precipitously as the battery reaches the end of its service life. Therefore one cannot expect to rely on the low battery warning system built into the AV-OS. Battery depletion may happen within days after a card was programmed and tested. Thus even if a

---

<sup>17</sup> The reports are available from at the URL <http://voter.engr.uconn.edu/voter/reports/>.

<sup>18</sup> T. Antonyan, N. Nicolaou, A.A. Shvartsman, and Th. Smith. Determining the Causes of AccuVote Optical Scan Voting Terminal Memory Card Failures, *Proceedings of the 2010 USENIX/ACCURATE Electronic Voting Workshop (EVT/WOTE 2010)*, Washington, DC, August 9-10, 2010.

card is successfully programmed, it can fail before it is tested prior to an election, or at any time after it is successfully tested. A new non-volatile (battery-less) memory card was recently developed by the vendor. Once tested, it is expected that a pilot deployment of the new cards in Connecticut will occur in the near future. The use of the new card should eliminate the major cause of memory card failures.

## **5. On Certification of Electronic Voting Equipment**

Optical scan voting technology offers a Voter Verified Paper Audit Trail (VVPAT) that currently presents a clear advantage over Direct Recording Electronic terminals (DRE). VVPAT enables hand counted audits to be performed after the election. A combination of comprehensive technological audits and hand counted audits can prevent electoral process failures and substantially increase confidence in the election outcome.

The complexity and size of election systems and their dynamic nature due to the software they use, preclude any absolute guarantees of security, integrity, correctness, fault-tolerance, and performance. Testing and certification notwithstanding, the only current way to confirm that the voter-verified paper ballots are correctly tabulated by electronic means and that the results are correctly reported is to hand count the ballots. In February 2006, a report commissioned by California's Secretary of State found that a certified compromised optical scanner would produce results that election officials and voters would not recognize as false: "There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots."<sup>19</sup>

While it is tempting to view a voting terminal in isolation for the purpose of testing, it is critical to view the entire system formed by hundreds (or even thousands) of voting terminals (and ballot marking devices, if any) distributed over a large geographical area and ultimately interacting with a single central system, e.g., EMS (Election Management System), for the preparation of the election and the tabulation of the results. It is therefore a large, complex distributed system (even if it is only sporadically interconnected, e.g., by means of programmed removable media devices).

---

<sup>19</sup> California Voting Systems Technology Assessment Advisory Board (VSTAAB), Security Analysis of the Diebold AccuBasic Interpreter, February 14, 2006.

Relying on EMS to perform central tabulation has its risks. EMS software is normally installed on general purpose computers and it is beyond the state-of-the-art to be able to reason about the correctness of the substantial amount of software in EMS and its computing environment. The risks are not hypothetical, for example, a Premier advisory note alerted EMS users that precinct memory card data uploads can be flagged as successful when in fact upload of data failed (ironically, the vendor stated that this may be due in some cases to a conflict with anti-virus software running on the EMS computer).<sup>20</sup>

Attempting to verify and certify an optical scan terminal without at the same time verifying and certifying all involved systems, including EMS, provides a false sense of security. It is important to reiterate that one cannot rely on the self-test features provided by any software system because one can never trust software to test or audit itself (cf. relying on a corporate entity to perform self-audit). Independent testing and certification addresses only a part of this concern, for testing cannot guarantee correctness. In November 2006, scientists at the National Institute of Standards and Technology (NIST), the agency that writes the federal voting system standards and advises the United State Election Assistance Commission, found that unless a software system was built to be secure and reliable to begin with, “experience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible”<sup>21</sup> and therefore testing of software-based voting systems cannot guarantee accurate and reliable election results.

A “certified” software-based voting machine can still be programmed to alter itself before, during, and after the election or can be subsequently manipulated with no ability for election officials or observers to perceive that the voting system has been compromised. Malicious coding can evade certification testing; the testing cannot guarantee to reveal that the code has been compromised. A certified software-driven voting system can be programmed to give the false appearance that it is in proper working order, when in fact it has been compromised.

---

<sup>20</sup> PREMIER ELECTION SOLUTIONS, Product Advisory Notice, GEMS versions 1.20.2 and earlier, Revision: 1.0 Date: 08-19-2008.

<sup>21</sup> National Institute of Standards and Technology report on computerized voting systems, NIST, <http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf>.

Lastly, software systems are perpetually revised, extended and corrected. Each change, in principle, must trigger a complete new regression test, test of the changed or corrected functionality, and complete re-certification. Even if this is done, the operation of a software system can be completely changed if new data and code are added – this is in fact the case with removable memory cards that are programmed for each voting terminal before each election. The conclusion is that systematic auditing, both hand counting and technological audits, is necessary to protect the integrity of the electoral process conducted with the help of computerized election systems.

## **6. Discussion**

In this article we provided an overview of the electoral process in the State of Connecticut, which integrates the use of optical scan electronic tabulators. The deployment of electronic technology in the State required the revision of the electoral process with the focus on its technological integrity and security. We covered the most visible new elements of the revised electoral process, viz., hand count audits in 10% of randomly chosen districts, and technological audits, both before and after the elections. These auditing procedures are specifically designed to enhance the integrity of elections conducted using optical scan technology. In addition to helping ensure safe use of technology in elections, these audits also help monitor adherence to the established policies and procedures in each election. Our experience shows that this approach is practical, and we are continuing to refine and enrich the auditing procedures that are now routinely used in Connecticut.