Is Technology the Answer? Software Quality Issues in Electronic Voting Systems

Duncan Buell and Gregory Gay
University of South Carolina
buell@cse.sc.edu, greg@greggay.com

Abstract

Casting a vote is the primary means by which citizens can influence their government. Following the passage of the Help America Vote Act (HAVA) in 2002, a surge in the use of electronic voting systems occurred. Although hand-marked paper is returning to use, the replacements in many jurisdictions for these aging electronic systems are also electronic. Given the serious nature of elections, electronic voting systems must be trustworthy, and their engineering must be held to rigorous standards.

We have had the opportunity, over the past eight years, to observe and analyze the use of electronic voting systems in the state of South Carolina. Our observations of such systems in the field have yielded serious usability, software, and hardware quality concerns, ranging from procedural errors resulting from poorly-designed systems, to system faults that ignore or miscount votes, to timestamp anomalies and malformed output. Given the importance of elections, and the inherent risk in the use of current electronic voting systems, we question the wisdom of using such systems until they are held to standards comparable to those used in other regulated, *safety critical* domains.

Keywords: Electronic Voting Systems, Software Quality, Usability

1. Introduction

Elections are one of the most important functions of an effective government, and casting a vote is the primary means by which citizens can influence

the decisions and direction of their government. Given the increasing use of computing for all of life in a modern society, there is a natural tendency to believe that *electronic voting systems* are the answer to the complicated process of conducting elections. These specialized cyberphysical systems are designed, theoretically, to allow secure and private election participation—reducing the need for human intervention in the election process, and by extension, reducing the potential for human error [11].

A well-established notion in Software Engineering communities is the *safety critical system*—a system where any fault in the source code or visible failure in operation has the potential to lead to loss of life or significant loss in property or material wealth [23]. Because of this risk, the engineering of such systems is a serious, rigorous matter, often subject to strict regulatory standards [22]. Typically, analyses of safety critical systems focus on avionic systems [10, 13] or medical devices [15, 16]—systems that pose a clear, immediate risk to humans, equipment, or the environment if not properly engineered.

However, elections too are events with serious consequences for both participants and society-at-large. Actors around the world seek to destabilize regimes, and engage in electronic warfare to obtain their goal. Complicating the problem are two issues somewhat specific to elections—the requirement in most circumstances that the cast ballot not be identifiable as having come from a specific voter, and the problem that elections are, in many places, run as a distributed process in local polling places on an Election Day that is a one time event conducted at scale. The first of these makes it hard to know what ground truth is, and the latter means that it is virtually impossible to test such systems under operational conditions. *Given their importance, however, electronic voting systems should be trustworthy, and their design and implementation should be held to rigorous standards.*

To date, there is significant evidence that electronic voting systems are not trustworthy. Such systems have been analyzed thoroughly from the perspective of security [2, 4, 5, 9, 19, 29], and we will go into some detail on these in Section 3. Concerns have also been raised about the usability of such systems [3].

There is much that can be learned about electronic voting systems and their use by election officials by performing a critical analysis of the software quality of such systems *in the field*. We have had the opportunity, over the past eight years, to observe and analyze (albeit indirectly) the use of such systems in the state of South Carolina. South Carolina votes statewide primarily on paperless ES&S iVotronic Direct Recording Electronic (DRE) machines. Following a highly publicized and highly anomalous outcome in the South Carolina statewide Democratic primary in June 2010, the first author, along with others and under the aegis of the League of Women Voters of South Carolina, undertook to examine the election results based on data obtainable through the Freedom of Information Act [7]. We have continued this analysis with each biennial election to date. In this report, we present the analysis of this data. Some of our observations include the following:

- Procedural errors, errors in the collection and preservation of election data, and erroneous output that could be addressed through usability improvements in the systems.

- Explicit event codes included in system logs with no developer-provided explanation—a threat to usability, system correctness, and verifiability of the results.

- Software quality issues, including missing log data, vote count discrepancies, multiply counted votes, ignored votes, incorrect vote tallies, and timestamp anomalies—including faults that have not been fixed or changed in behavior over time.

- Hardware failures, including screen calibration and timing issues, that have increased over time as these systems age.

Our analysis is not exhaustive. We make no claims that we have uncovered all possible problems or complications—only the anomalies that have presented themselves in the data. Our observations nonetheless raise multiple concerns

about the software quality, hardware quality, and usability of the systems relied upon in actual elections.

Given the importance of such elections, and the inherent risk in the use of current electronic voting systems, we question the wisdom of using such systems in their current form. Rather, we recommend that such systems be held to standards comparable to those used in other regulated, safety critical domains before they be trusted even on the scale that they are already deployed in the United States and other countries.

2. Background

2.1. Electronic Voting Systems

The 2000 presidential election, with the famous "hanging chad" problems in Florida[1], led to the passage of the Help America Vote Act (HAVA). The HAVA legislation provided substantial federal funds to the states for the purpose of improving elections by modernizing the equipment used for casting ballots.

This federal funding was use by a number of states to purchase direct-recording electronic (DRE) voting computers—voting systems that record votes by means of a ballot display with mechanical or electro-optical components that can be activated by the votes through a touchscreen or buttons [27]. The choice of equipment is, in most states, left up to the counties making up the state. Counties can generally select from a list of options approved by a state agency that reports to the Secretary of State. Some state regulations have required DRE computers to produce a paper trail, usually resembling a long cash register receipt, that can be viewed by the voter before casting the ballot. Six states, after HAVA, chose to have a uniform voting system that was all electronic with no paper trail. Georgia and Maryland purchased equipment from Diebold (which became Premier, and then Dominion); South Carolina chose

[1] Votes are often recorded on paper ballots by punching a hole through a chad—a perforated spot in the ballot. In the 2000 presidential election, many ballots used in Florida had chads that were not fully removed, leading to votes that were not counted.

equipment from ES&S; New Jersey and Louisiana chose equipment from Sequoia. In other states there was, and often still is, a mixture of systems used, and there are even counties that have used multiple systems in the same elections. As of this report, the market is dominated by ES&S, Hart Intercivic, Dominion, Clear Ballot, and Unisyn—a small list of vendors. We are focusing on the iVotronic DREs and the Unity software package run at county headquarters, from ES&S. This is the system that is used statewide in South Carolina and is used in counties in 15 other states [27].

2.2. The South Carolina Election System

As of 31 December 2018, South Carolina has 3,143,018 registered voters spread across 46 counties in 2269 voting precincts. The largest three counties are Greenville, Charleston, and Richland, with 308,092, 272,991, and 248,352 registered voters in 151, 182, and 149 precincts, respectively. The smallest are Allendale and McCormick, with 7,172 voters and 9 precincts and 7,005 voters and 11 precincts, respectively [26].

We note that voters can request a paper absentee ballot by mail (if they meet one of several requirements for absentee voting) and to return that ballot by mail. We have not analyzed any of the paper absentee ballots. These normally are a small percentage of the total; in November 2018, only 3.7%, 7.4%, and 5% of the total votes in Greenville, Charleston, and Richland counties were cast on paper. "Absentee in-person" voting is done on the iVotronics (which we will refer to as "terminals", following the language in the vendor's manual for use), usually at the county election headquarters.

Voting is, thus, largely done on the 12,000 or so iVotronic terminals; state law nominally requires one terminal for every 250 voters in each precinct, although this requirement is often not met by the counties. (The statewide number of registered voters and of terminals is about 250 per terminal, but the need to have at least two in each precinct causes many larger precincts to fall below the required number.) The terminals are distributed to the precincts prior to

Election Day. Election Day runs from 7:00am to 7:00pm, with voters permitted to vote after 7:00pm if they are in line at 7:00pm.

The official protocol for use is that each terminal is opened for voting on Election Day using a "supervisor" PEB (Personalized Electronic Ballot). The PEBs are handheld devices a little smaller than a paperback book. Each precinct is to have one supervisor PEB for opening and closing the terminals and several other PEBs used by the pollworkers to open the terminal to receive one vote each time a voter uses the terminal. The PEBs are intended to be distinguished by rubber bands of different colors that run around the outside.

The PEB fits into a recess in the terminal and makes connection with the terminal via an infrared link. At the end of Election Day a terminal should only be closed and its votes collected by the same PEB that opened it. When the terminal is closed, its vote totals (but not the individual cast vote record) are copied into the PEB; at the end of Election Day, there should be one supervisor PEB that has opened and closed each terminal and that has accumulated the vote totals from each terminal. The PEBs are returned to county headquarters where the vote totals are accumulated into a county total.

When the terminals are closed, the "event log" for that machine and the "vote image file" of the cast vote record of individual ballots are written to a CompactFlash memory card slotted into the back of the terminal. The memory cards are then to be pulled from the terminals, placed in a plastic bag similar to a bank deposit pouch, and returned to county headquarters, where the vote image and event log files are to be uploaded into a master file as part of the canvass [24]. South Carolina is a precinct-count state. A "zero-tape" is produced for each terminal when it is opened on Election Day and then the vote totals for each candidate are printed on an exit tape when polls and the terminals are closed. Both tapes are to be posted on the door of each polling place.

3. Related Work

There has been extensive analysis done on the various electronic voting systems available for sale and use in the United States. The most prominent of the official analyses are the California Top-To-Bottom-Review assembled for Secretary of State Debra Bowen of California in 2007 [8], the EVEREST report assembled for Secretary of State Jennifer Brunner of Ohio and released in December 2007 [19], the report assembled for the Secretary of State of Florida and published in 2007 [29], and two Government Accountability Office publications [17, 18].

The latter three reports were assembled after a significant undervote for U. S. House of Representatives using ES&S iVotronics in Sarasota, Florida, in 2006[2]. The scope of the Florida studies were very narrow and limited to, at the most, determining whether the iVotronic itself could have been responsible for the undervote. Although the scope was narrow, the report for the Secretary of State was strongly negative in an appendix when discussing the password mechanisms used to get access to the iVotronic [29, pp. 66ff].

The California report examined voting systems from vendors Diebold (which became Premier, and then part of of ES&S, and is now a part of Dominion), Sequoia, Hart, and ES&S (although it was the InkaVote system from ES&S and not the iVotronic), and the report was primarily on security vulnerabilities in the software either in the voting computers or in the central computers [8].

The EVEREST study looked at Hart and Premier/Diebold, but importantly for our purpose, it contained a detailed study of the ES&S iVotronic— specifically of the same software versions used until the 2018 Primary in South Carolina, as was confirmed by the South Carolina State Election Commission [28].

Although the EVEREST study was again primarily a study of security vulnerabilities, there is significant commentary about vulnerabilities that would

[2] An undervote occurs when a voter chooses not to vote for any candidate for a particular contest.

result from low quality in the software. A main conclusion is that the "ES&S Unity E[lection] M[anagement] S[ystem], iVotronic DRE and M100 optical scan systems lack the fundamental technical controls necessary to guarantee a trustworthy election under operational conditions." [19, p. 29]. Relevant to our discussion here is that among the "several, pervasive, critical failures of the ES&S system" is: "Failure to follow standard software and security engineering practices — A root cause of the security and reliability issues present in the system is the visible lack of sound software and security engineering practices."

A significant difference between the studies discussed and our own is that we have not been permitted access to the source code. Our analysis is instead based on characteristics of the output that would suggest faults within the source code and hardware.

Following incorrect results in the 2008 Presidential Preference Primary in New Jersey[3], and after a protracted legal process regarding proprietary software, the Sequoia AVC Advantage was examined [2]. In addition to system flaws that could lead to the introduction of fraud or of malware, it was found that user interface errors could lead to the failure properly to count votes.

In addition to the official and institutional studies described above, the Diebold/Premier/ES&S/Dominion AccuVote TS and AccuVote TSX DRE have been extensively studied in less official ways [9]. We remark that in 2017 and in 2018 the DEFCON conference had a voting village with hardware to be hacked, and that reports have been issued [4, 5].

4. Case Study

Given their importance, electronic voting systems must be trustworthy, and their engineering must be held to rigorous standards. In essence, we believe that voting systems should be treated as a form of critical system like medical devices, automobiles, or rockets. Past investigations have raised questions about

[3]The totals of votes for individual candidates of the two major parties was not the same as the reported total of votes for any candidate of that party.

the security and usability of such systems, implying that they are not developed to the standards of critical systems [8, 19]. We have had a unique opportunity to examine how these systems perform in the field, in elections held in the state of South Carolina.

South Carolina votes statewide primarily on paperless ES&S iVotronic Direct Recording Electronic (DRE) machines with initial tallying done at the precinct level and then final tallying done for each county using the Unity software system running on a Windows computer at county headquarters[4]. The Unity software suite comprises several programs [19], including:

1. The Election Data Manager, that initializes a central database with jurisdiction, voter, and candidate information;
2. Image management software to design the appearance of the ballots;
3. The Election Reporting Manager that collects and tallies election results.

Prior to the 12 June 2018 First Primary, the the iVotronic terminals were running software version 9.1.6.0 and version 7.1.2.1 of the Election Reporting Manager; during the spring of 2018 all counties upgraded to iVotronic software version 9.2.0.2 and Election Reporting Manager version 7.7.1.0. A much more detailed description of the software can be found in the EVEREST report [19].

The system as used in South Carolina is entirely electronic; there is no auditable primary data (such as paper ballots), but there are several audit trail files that are produced by the software of the ES&S system. Probably unique in the United States, however, South Carolina not only declares all election data (including the cast vote record, in an anonymized order of votes) to be public record, but pro-actively publishes that data on the State Election Commission website [25]. This permits a third-party analysis that probably could not be done in any other state. In addition, the fact that South Carolina votes statewide on a single voting system makes statewide comparisons possible.

[4] The iVotronic Voting System is a registered trademark of ES&S. Election Reporting Manager is a trademark of ES&S.

Following a highly publicized and highly anomalous outcome in the South Carolina statewide Democratic primary in June 2010, the first author, along with others and under the aegis of the League of Women Voters of South Carolina, undertook to examine the election results based on data obtained (at that time) through the Freedom of Information Act (FOIA) [7]. We have continued this analysis with each biennial election to date.

We now have data from the general elections of 2010, 2012, 2014, 2016, and 2018, as well as for other elections, including the First Primary held on 12 June 2018. We will refer to "the 2012 data", for example, in what follows, except for the year 2018. Since there was a software upgrade in the spring of 2018, prior to the 12 June 2018 First Primary, we will include the data from the First Primary as well as from the General Election of 2018; by doing this, we get more data about what might have changed from one version of the software to another. We will thus refer to "the 2018 Primary" and "the 2018 General Election".

The software and hardware used in South Carolina are proprietary and, thus, not directly observable by third parties. However, the EVEREST report [19] written for the Secretary of State of Ohio, provides analysis that guides our own. Even without knowing the internal details, there is much that can be learned about the election system and about its use by election officials by performing a critical analysis of the software quality of such systems *in the field*. We are interested in the insights that eight years of election data can offer about the software failures observed in the field, how such issues have evolved over time, how hardware deterioration impacts the correct functioning of such systems, and whether software failure can be induced by user mistakes—particularly as such systems are often activated and administered by volunteers. In particular, out investigation is framed by the following research questions:

1. Does the captured election data indicate the presence of **software** faults that result in visibly incorrect system behavior?
2. Does the captured election data indicate the presence of **hardware** faults that result in visibly incorrect system behavior?

3. Does the captured election data indicate misuse by human administrators that could be the result of mistaken assumptions about system use that are induced by the design of the system?
4. Over time, are there software faults that have been corrected, not corrected, exacerbated, or newly induced by changes to the system codebase?
5. Over time, what impact has aging hardware had on system correctness?
6. Over time, have usability issues been corrected or introduced by changes to the system codebase?

4.1. Election Data

When devices and data are returned to county headquarters, the vote totals from the PEBs are aggregated into a county total, and the event logs and cast vote records from each terminal are put into a county database.

We have generally used in our analyses four reports that are produced at county headquarters. These reports are considered public records by the state of South Carolina, and are posted on the State Election Commission (SEC) website following an election (see, for example, [25]).

The EL155 Vote Image File is the cast vote record. A sample of this—an actual ballot from the 2016 General Election—is presented as Figure 1[5]. An individual ballot begins with the line containing an asterisk and continues until the next line that has an asterisk. Each line contains, in order, the terminal serial number, the ballot style (in what are called "split" precincts, there will be voters in a given precinct who lie in different electoral jurisdictions; there are precincts in South Carolina, for example, with voters from two different congressional districts), the possible asterisk, the candidate's code number, and then the candidate name and the election contest. (Other ballot items such as constitutional amendments are also present, but we will write for brevity as if only candidates and elected positions were on the ballot.)

[5]This is not the ballot cast by the first author, but does happens to show a write-in for the first author. This shows that South Carolina considers the names of write-in candidates to be public record. Not all states take this position.

```
5134625    3     53 Calvin Chip Jackson                  CCL0009 County Council District 9
5134625    3     56 Jeff Laney                           Soil and Water
5134625    3     59 Lindsay Agostini                     SCH0002 School Board District 2
5134625    2 *   15 Peter Skewes                         PRESIDENT AND VICE PRESIDENT
5134625    2     23 Rebel Michael Scarborough            U.S. SENATE
5134625    2     30 Eddie McCain                         CON0002 U.S. House of Rep Dist 2
5134625    2     33 Mia McLeod                           SEN0022 State Senate District 22
5134625    2     37 Joe McEachern                        HOU077 State House of Rep Dist 77
5134625    2     41 W/I DUNCAN BUELL                     Sheriff
5134625    2     43 Jeanette W McBride                   County Clerk of Court
5134625    2     46 Gary Watts                           Coroner
5134625    2     49 Gwen Kennedy                         CCL0007 County Council District 7
5134625    2     56 Jeff Laney                           Soil and Water
5134625    2     63 Kay Harvey                           SCH0002 School Board District 2
5134625    2     65 Bill McCracken                       SCH0002 School Board District 2
5134625    2     69 Shelley Williams                     SCH0002 School Board District 2
5134625    3 *    6 Republican                           STRAIGHT PARTY
5134625    3     14 Donald J Trump                       PRESIDENT AND VICE PRESIDENT
5134625    3     19 Thomas Dixon                         U.S. SENATE
5134625    3     29 Joe Wilson                           CON0002 U.S. House of Rep Dist 2
5134625    3     34 Susan Brill                          SEN0022 State Senate District 22
```

Figure 1: Sample Text from an EL155 File

Candidates are identified in the terminals only by code number and not by name, and the code number is then used to attribute a vote to a candidate when the tallying is done at county headquarters on the Unity software. From the EL155 report we can connect terminals by serial number with precincts, and we can determine the actual vote totals for each candidate.

The EL152 Event Log File is the record of events from each terminal. A sample of this is presented as Figure 2. This sample comes from Chester County in the 2018 Primary. The first entry is the terminal serial number. If the event was triggered by use of a PEB, that PEB's serial number appears next as well as the type of PEB. There is a timestamp, an event code number, and then the expanded English text of what event is indicated by the code number. We note that the existence of votes, with timestamps, are events that are recorded, in this example with code 0002900. Some events lack an expanded English definition, simply being noted as "UNKNOWN" events. (We will discuss this more in Section 5.)

```
5132179  130966  SUP   2018-05-23 13:57:41   0001607 Clear-n-test terminal flash successful
                 SUP   2018-05-23 13:58:20   0000116 Select: Configure Terminal
                 SUP   2018-05-23 13:58:26   0001650 Terminal - exited service menus
         123887  SUP   2018-05-23 14:02:14   0001001 Confirm PEB ballot failed by user
         147244  SUP   2018-06-12 06:55:17   0001303 Transfer PEB vote data to terminal
         143916  SUP   2018-06-11 19:32:43   0001319 Update PEB's terminal record
                 SUP   2018-06-12 06:55:23   0000019 UNKNOWN
         143400  SUP   2018-06-10 09:25:04   0001024 UNKNOWN
         146732  SUP   2018-06-10 18:31:29   0000066 UNKNOWN
         146728  SUP   2018-06-10 09:25:24   0001882 UNKNOWN
         146732  SUP   2018-06-10 18:31:58   0000019 UNKNOWN
         146728  SUP   2018-06-10 09:19:32   0001920 UNKNOWN
         147244  SUP   2018-06-12 06:58:49   0002006 Print task was cancelled
                 SUP   2018-06-12 06:58:53   0001672 Terminal Opened
         123887  SUP   2018-06-12 07:05:22   0000621 Warning: Terminal reset from voting
                 SUP   2018-06-12 07:07:12   0002900 Vote cast by voter - Visual
```

Figure 2: Sample Text from an EL152 File

From the EL152 report, we can connect terminals with the PEBs by serial number that opened and closed the terminals, and we have events recording the existence (but not the essence) of the votes. In addition, we have records of maintenance work (such as calibrating the touchscreens) and reports from the terminals of hardware or software errors.

The EL68A System Log, a sample of which is presented as Figure 3, is the system log from the Windows computer running the Unity software at county headquarters. From this report, we can verify that the databases were cleared prior to an election (it does happen that test votes remain in the database; this is a practice that is sloppy but does not usually cause problems in the final tallies). We also see reference via serial numbers to PEBs and collection of votes and of the import into the central databases of the EL152 event log and EL155 cast vote records from each terminal. At least two other significant messages, indicating errors in the configuration of the election, will be displayed in the 68A, and will be discussed in Section 5.

The EL30A report is a report for each county, precinct by precinct, of the vote totals that have been aggregated for the county. South Carolina also

```
SYSTEM LOG LISTING                                    Richland County
                                                      Statewide General
                                                      November 6, 2018
RUN DATE:11/09/18 06:09 PM
ELECTION ID: 40110618

USER DATE   TIME     SYSTEM ACTION OR ERROR INFORMATION                COUNTED INFORMATION

   11-07    01:08 am 5268-Bypass duplicate record
   11-07    01:08 am 5268-Bypass duplicate record
   11-07    01:08 am 5268-Bypass duplicate record
   11-07    01:10 am EXIT PROCESS PRECINCT RESULTS MEDIA
   11-07    01:11 am CANVASS - BLOCK STYLE WAS PRINTED TO EL119.LST
   11-07    01:12 am PRECINCT REPORT WAS PRINTED TO EL30.LST
   11-07    01:18 am                                                 PRC 0750 RESET  (GRP 05)
   11-07    01:18 am                                                 PRC 0751 RESET  (GRP 05)
   11-07    01:18 am PRECINCT REPORT-GROUP DETAIL WAS PRINTED TO EL30A.LST
   11-07    01:22 am START COLLECT AUDIT DATA FROM COMPACT FLASH
   11-07    01:22 am STOP COLLECT AUDIT DATA FROM COMPACT FLASH
   11-07    01:23 am START COLLECT AUDIT DATA FROM COMPACT FLASH
   11-07    01:23 am STOP COLLECT AUDIT DATA FROM COMPACT FLASH
   11-07    01:23 am START COLLECT AUDIT DATA FROM COMPACT FLASH
   11-07    01:24 am Audit Data collected for V5109433
   11-07    01:24 am V5109433.SPV created
   11-07    01:24 am V5109433.COD created
   11-07    01:24 am
   11-07    01:24 am Audit Data collected for V5127871
   11-07    01:24 am V5127871.SPV created
   11-07    01:24 am V5127871.COD created
   11-07    01:24 am
   11-07    01:24 am Audit Data collected for V5129902
   11-07    01:24 am V5129902.SPV created
   11-07    01:24 am V5129902.COD created
```

Figure 3: Sample Text from an EL68A File

publishes other reports, but this one has been the most useful, since it has votes by precinct, by contest and candidate, and by means of obtaining votes (from PEB collection from terminals, from paper absentee counts, and directly

from the EL155 cast vote record on the memory cards if a terminal could not be closed and the votes had to be collected in a manner different from the standard protocol). Although this report is somewhat tedious to parse, because it seems to be intended for a fanfold-paper printer from the 1970s, it is not actually difficult to extract the needed information. We note that prior to the "upgrade" for the June 2018 primary, there were a number of slightly different output formats for this report from the different counties, but now all counties except two seem to have standardized on a single format—correcting a potentially serious issue.

4.2. Analyzing the Data

We began our third-party analysis in 2010 with attempts to determine what one could infer from looking at the election data. That first analysis showed that, at that time, much of the election process in South Carolina was deeply flawed. Several counties were unable to provide data, even though the Help America Vote Act (HAVA) regulations would have required that data to be preserved for 22 months. We asked twice by FOIA request, for example, for data from Charleston County, and were provided each time only with data for about 10% of the votes cast.

Over time, as we have discovered problems, we have added to the reporting of "exceptions" that indicate the possibility of problems. Much of our analysis is, by nature, a reconciliation of the data with itself. From the EL155, we can associate iVotronic terminals with precincts and can count votes for candidates. From the EL152, we can associate terminals with the PEBs that open and close and collect vote totals, and we can count the number of votes recorded by each terminal. From the EL68A, we can verify by serial numbers that PEBs that have collected vote totals have had their totals uploaded into the central database, and we can verify that memory cards for each terminal have had their data uploaded into the central database.

The 2012 General Election in Richland County (home to the state capital, Columbia, and the University of South Carolina) was a debacle in which voters

stood in line for as long as seven hours and the last votes were cast after midnight, more than five hours after the polls closed. Conspiracy theories about biasing a tax referendum were rife and a lawsuit went all the way to the South Carolina Supreme Court before being rejected. The county election commission contracted with an attorney to produce a report on what happened, and the attorney contracted with the first author for an analysis. We were able to demonstrate through simulation that in fact the problem was simply that too few terminals had been allocated for the election and also that terminals were failing, leading to an additional decrease in resources. By looking at the numbers of votes cast on each terminal in each 15-minute interval, we were able to pinpoint possibly-failing terminals. A terminal that collected few or no votes in several intervals, when other terminals in the precinct were steadily collecting votes, was likely having problems, and in many instances these problems showed up as events recorded in the EL152 log [6]. Our analysis showed [12] that mismanagement was a more likely cause than intent—for this quadrennial election, Richland County left one-third of its iVotronic terminals in the warehouse.

We now have data from five successive biennial elections and the First Primary held in June 2018, and we have data from the original software installed in 2004-2006 and from the upgraded software installed in the spring of 2018.

Our programs were originally written in Java. A second version was written in C++, and the current versions are written in Python and comprise about 3800 total lines of code. The source code of our analysis framework is publicly available from `https://github.com/dabuell/SCElectionAnalysis`. South Carolina election data is also publicly available from
`https://www.scvotes.org/election-audits-south-carolina`.

The data for all of South Carolina for the 2018 General Election totals to approximately 2.5 Gigabytes, and processing this data takes only minutes on a modern desktop computer. This code has also been used by two different research groups outside South Carolina who have successfully analyzed other data without our intervention.

In addition to South Carolina, we have also analyzed data from Venango County PA, Hidalgo County TX, Jefferson County CO, Mecklenburg County NC, and Ellis County KS. The basic software structure has been the same in all cases, although minor tweaks to our software have been necessary (usually just minor annoyances like extra header lines on every output "page"). Because of this we believe we can draw conclusions about the ES&S election system generally and not just the system as installed in South Carolina.

5. Results

Our goal with this analysis is to understand the in-the-field behavior of the ES&S election system by analyzing the data it produces and by looking at how the system is used by its intended users, namely the election officials and the volunteer pollworkers in the precincts on Election Day. Through this analysis, we hope to understand the implications of the software quality, hardware quality, and usability of this system—and how these factors have changed over time.

Our analysis itself has changed over time. Much of our earlier analysis focused on use of the system; we contend that if technology cannot be used effectively by those who are intended to use it, then it is the technology, and not the users, who are at fault. With this point of view, an analysis of mistakes made by the users can be viewed as a measure of the effectiveness of human factors considerations in the design and production of the system.

With the upgrade in Spring 2018 to new software both in the terminals and in the computers at county headquarters, we can see whether known problems and faults were fixed in the upgrade. Unlike many consumer systems, whose faults can be fixed in routine updates, many states require that an election system be certified—often by one of the handful of testing companies. This severely limits the ability to fix faults rapidly, but we expect this also permits a measure of the vendor's quality control and fault management; if updates happen infrequently and only with the concomitant expenses of being tested independently, one would expect known faults to have been corrected in the

updates that are released. This assumption, thus, allows an assessment of the vendor's quality control process.

In this section, we explain anomalies detected in the election data, categorized as usability, software quality, or hardware quality issues.

5.1. Usability Issue: Procedural Errors, and Errors in Collection and Preservation of Election Data

The ES&S election system is, by any standard, a complicated computer system. It comprises, according to the EVEREST report [19], 515,000 lines of code in nine different programming languages on five different hardware platforms. Our original analysis in 2010 began with no assumptions; it was an exploratory look at the data to see what could be seen.

We began with FOIA requests of several counties for the 2010 election data. Our analysis then showed that many counties either were having trouble using the system or, in contravention of the HAVA requirements, failing to retain the data. The most significant result was the discovery that more than a thousand votes cast in Richland County had not been included in the official count. In one precinct, six of the eight terminals had never been closed. In spite of exit tapes with "MACHINE NOT CLOSED" in capital letters, and in spite of a sign-in book with more than a thousand signatures, the precinct reported only 254 votes cast, 772 votes were not counted, and the error was not detected until a week after the results were certified.

In a second precinct in Richland County, six terminals were opened and closed with two PEBs and not just one, and the 355 votes from the second PEB were not included in the certified count. Though these were the largest instances of failing to count all the votes, they were not the only ones; similar problems occurred in other counties.

After a 14 February 2011 press release from the League of Women Voters, the SEC obtained from the counties what data the counties held and engaged a programmer to write programs equivalent to ours.

The 2010 data showed a profound inability of the counties to use the election system, or else a disinterest in collecting and saving (as legally required by HAVA) the data for later reconciliation. Our FOIA requests to Charleston County resulted in receipt of only about 10% of the vote data; the state later obtained only about 75% of the data. In that county, there were 104,087 certified votes, but the EL152 obtained by the state has data for only 83,009 and the EL155 has data for only 75,991; data to support the existence of nearly 30,000 certified votes is just missing.

Similarly, in Colleton County, with a new election director, neither the county nor the state were able to produce correct vote tallies. Reports were of votes added in twice (according to the vendor's manual, the screens for incrementing the vote count and for replacing votes with new counts are nearly identical) and similar mistakes. In Horry County, there were 71,211 certified votes. Our data received via FOIA requests contained 59,079 votes, with data missing for 48 precincts. The EL155 file obtained by the state was mysteriously missing all data for (a different set of) 25 precincts in the middle (by number) of the list of precincts; that data showed 66,651 votes in the EL152 and 53,483 in the EL155.

The data from 2010 and 2012 showed a number of procedural errors or oversights. Terminals were not closed. Memory card data was not collected. Votes were not counted because multiple PEBs were used to open and close terminals in precincts. In one instance, the absentee votes were added in manually (this is reported in the EL68 report that is also posted on the state's website), and none of the seven candidates in a school board election were assigned the correct vote count, although the order of the candidates was correct.

What became apparent is that the software system seems to do little to assist the election officials in determining that they have finished with the tallying process. Richland County, for example, with about 250,000 registered voters and 150 precincts, sends out about 1000 terminals, each with a CompactFlash memory card, and about 1000 PEBs for a biennial election. With that many devices, it would be useful to record, by serial number, the devices sent into the

field and the devices returned home safely, but there seems to be no ability to do this. In smaller counties, the problem of managing the hardware is less of an issue, but on the scale of Richland County, software to manage the process should be included in the package. This would be even more necessary in larger states and in larger counties elsewhere in the country. We have observed, for example, that the memory cards seem to be treated as interchangeable commodities and often are not labelled; this means that the only way to determine which card might have come from which terminal is to slot the card into a reader and look for a terminal serial number in the file names (see Figure 3). Some counties manage to maintain an assignment of terminals to precincts from one election to the next, but many do not, adding to the problem of managing devices.

With the 2014 biennial election, the SEC required counties to submit data and ran its reconciliation programs before it would permit results to be certified. By the 2016 General Election, the *process* of conducting elections seemed to have stabilized. In only a handful of precincts were there problems of data missing or not collected. The main problems with the system no longer seem to be an inability of the intended users to use the system. Nearly all the votes seem to be tallied correctly and the data collected and preserved, and we attribute this to the after-election checking by the SEC. There are, however, still serious mistakes made that lead to votes that are not counted, or counted for the wrong candidate, or counted more than once.

It should be pointed out that the ES&S system does have redundancy features that other election systems do not, and the South Carolina transparency with respect to the data is commendable. The Diebold AccuVote system, for example, only stores one copy of the data in its internal memory and then one copy on the removable memory card [9]. In contrast, the fact that the EL152 log records the existence of votes, the EL155 records the votes themselves, and the totals are collected by the PEBs in a third path, permits through the partial redundancy a reconciliation of the data with itself and a checking for errors. This, in itself, is a good thing, but it is clear from the errors committed by the

users of the system (election officials and pollworkers) that there are insufficient software interventions to ensure that mistakes are not made.

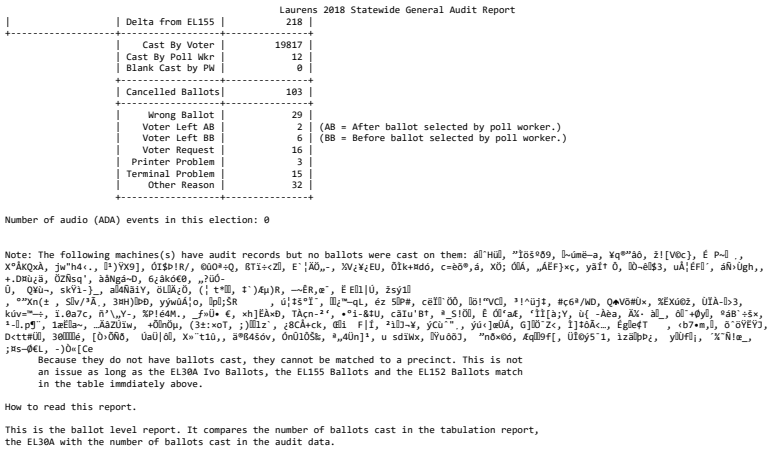
We argue that the insufficiency of software to check and double check the process is a flaw in the design. Pollworkers are frequently retired citizens; Election Day begins at about 6:00am and doesn't end until 8:00pm or so. This makes for a long and tiring day, and of course, Election Day is a one-time event that cannot be postponed. A system in support of such a process needs to be completely bulletproofed and made failsafe, and the ES&S system appears to be lacking in this regard. One of our major complaints through the years has been that the South Carolina protocols for use of the election system seem to have been designed and produced as if best-case scenarios were the norm. In any use of computers, the opposite must be assumed.

5.1.1. Software and Usability Issue: Inattention to Garbled Data

Although there has been substantial improvement in the gathering, preserving, and reconciliation of the the election data, problems clearly still exist, and some of the problems are indicative of either unjustified trust in technology or a too-quick abandonment of thorough analysis when the technology fails.

Laurens County in the 2018 General Election is an example of this and highlights a shortcoming in the SEC's analysis. The EL152 file seems to have been garbled near the end in its transmission to the SEC, due to an unknown software or hardware fault. The malformed output, manifesting as character codes not corresponding to legitimate ASCII characters, break our analysis program.

We note, however, that by looking at the Commission's report for Laurens County, we can argue that the state's programs and its analysis are highly suspect. The Laurens County report contains the page shown as Figure 4. It is unlikely that reasonable analysts would have read this page and not known that something was wrong and should be looked into. Yet, there is no acknowledgement in the report to indicate a recognition of the error that derives directly from the malformed output in the EL152.



Laurens 2018 Statewide General Audit Report

	Delta from EL155	218
	Cast By Voter	19817
	Cast By Poll Wkr	12
	Blank Cast by PW	0
	Cancelled Ballots	103
	Wrong Ballot	29
	Voter Left AB	2
	Voter Left BB	6
	Voter Request	16
	Printer Problem	3
	Terminal Problem	15
	Other Reason	32

(AB = After ballot selected by poll worker.)
(BB = Before ballot selected by poll worker.)

Number of audio (ADA) events in this election: 0

Note: The following machines(s) have audit records but no ballots were cast on them:

Because they do not have ballots cast, they cannot be matched to a precinct. This is not an issue as long as the EL30A Ivo Ballots, the EL155 Ballots and the EL152 Ballots match in the table immdiately above.

How to read this report.

This is the ballot level report. It compares the number of ballots cast in the tabulation report, the EL30A with the number of ballots cast in the audit data.

Page 3

Figure 4: The SEC report for Laurens County, 2018

We manually removed the offending lines from the 152 file and then ran our program again. This allowed an analysis that had some obvious problems due to the missing data. We suspect the SEC's program (that was originally written in Java) might have been more forgiving with regard to reading bad characters than our Python program, and suggests that sometimes it's better to have programs fail and thus call attention to error conditions.

The malformed output also suggests an improvement that could be made to the electronic voting system as well. The system itself should perform an analysis of its data to detect malformed and other erroneous output. A system that must be trusted should do more to ensure either that its behavior is correct or that its users are made clearly aware when something is not correct.

5.2. Software and Usability Issue: Event Codes With No Explanation

An event in the iVotronic is recorded with a timestamp for when the event occurred, the PEB serial number if a PEB was used in the event (like opening and closing the terminal), and a code number for the event. In the EL152

report, the code numbers are accompanied by an English explanation, retrieved from a lookup table.

An indication about poor software quality in this election system can be taken from the fact that there are event codes that expand into the explanation "UNKNOWN". This means that a developer felt that an event was worth recording, but never finished entering an English explanation in the table for the EL152. It also means that neither quality control for the project nor management at ES&S ensured that all codes were expanded. This is a serious usability issue, as it hampers the ability of election officials to verify the integrity of data. It is also a serious software quality issue, as it prevents diagnoses and debugging of software faults.

We observed that eleven of the "UNKNOWN" event codes in the 12 June 2018 First Primary data do not appear in either the 2014 or the 2016 data. This suggests that either new codes were added for which sloppy practice resulted in no explanation in the table or that there were changes in the software that resulted in the triggering for the first time of already existing codes. The latter case is not encouraging, as that implies that no one noticed that prior sloppy practice was now newly exposed. These practices should not occur in a software production environment with proper quality control and testing, and further suggest the need for regulated development of these systems.

We note that code 0000180 was "UNKNOWN" in 2012 and 2016, but has become "Select: Collect PEB Audit Data" in the 2018 General Election data. If this is a new code, it suggests the creation of event codes without checking to see if the code number is already spoken for. If this is not a new code, then the existence of "UNKNOWN" codes was noted by someone on the development staff, but no one beyond that particular developer did anything about it.

We have seen, since 2010, a total of 84 different event code numbers whose expansion into English is "UNKNOWN". Of these, 42 appeared either in the 2018 Primary data or in the 2018 General Election data, or both. And 28 of the 42 appeared only in one of the two 2018 elections, that is, only in the new and "upgraded" codebase.

In addition to the "UNKNOWN" codes, we notice two codes in the data, 0000000 and 0001648, that have no English text expansion at all in the EL152 log. The former appears in 2016 and in the 2018 General Election, and the latter only in the 2018 General Election.

What is especially troubling is the frequency with which the "UNKNOWN" codes appear in close proximity to timestamp anomalies inside the terminal. We will discuss such anomalies shortly.

5.3. Software and Hardware Issue: Missing Log Data, Vote Count Discrepancies

We have observed a phenomenon in the 2018 Primary and the 2018 General Election that is an additional concern. For a small number of terminals and a small number of votes, the EL152 log ends abruptly and there are more votes in the EL155 cast vote record than there are 0002900 "Vote cast by voter" events in the EL152 log. We have seen situations before in which misbehaving terminals could not be closed and their votes were gathered by some other mechanism. It is apparently possible to flush the EL152 and EL155 internal data to the memory card without generating a "close terminal" event. This seems to have happened on occasion in the past.

What is new here is that an otherwise normal EL152 record ends abruptly, as if the last output buffer has not been written[6]. Invariably, these were instances in which the terminal was clearly failing. In these terminals, the log file ends abruptly, there is no record of closing, and there are fewer "vote cast" events (by one or two) in the EL152 than there are instances of cast votes in the EL155. In the 2018 General Election, this happens in Anderson, Darlington, Greenville, Greenwood, Richland, and Sumter Counties.

The number of votes involved is small, so we are not concerned about changes in the election outcomes from the small miscounts that are observed. What

[6]This is a common error in programming; the steady state process is to write the buffer in the loop when it fills, but when one runs out of data at the bottom the partially filled buffer needs to be written out by code outside the loop.

does concern us is the implication for software quality that comes from such anomalies, and the potential for small faults to compound into serious, subtle failures. We should not expect to see log files that are not complete; the purpose of a log file is to be a complete record of actions taken. We have not seen these anomalies prior to 2018, and we have not seen these anomalies related to a difference in the vote counts. What is of concern is the fact that this kind of unexplainable anomaly is often indicative, in software, of deeply hidden errors.

An example of this occurs with the misbehaving terminal in the 2018 Primary that resulted in votes being counted twice by the election officials (the double counting is described immediately below). The misbehaving terminal has four "vote cast" events in the EL152, but five votes are recorded in the EL155 and included in the certified count. The event log also has several events that indicate problems with the internal terminal memory and problems with the CompactFlash memory card.

5.4. Software Issue: Votes Counted Twice

In general, it seems that the process of conducting an election has improved greatly since we began analyzing the data in 2010. However, there are still some significant errors that we could probably attribute to the the complexity of the system. In Wallace Precinct in Marlboro County in the 2018 Primary, there were apparently 148 voters who had the distinct privilege of voting twice. This error was not caught by the county or the state, and the totals as reported are simply wrong. There was one terminal, serial number 5123479, that was (based on reading its event log) clearly failing. Instead of adding in just the five votes from that terminal into the totals, the other 148 votes from four other terminals in that precinct were added to the totals both from their memory cards and with the usual PEB-based process. Instead of 153 total votes in the precinct, the total was reported as 301 by incorrectly double counting the 148 to get 296 and then adding in 5 more from terminal 5123479.

One can imagine mechanisms that might prevent such double counting; some of these are more feasible than others in an election system. Since votes are sup-

posed to be anonymous, it might not be feasible (or legal, in some jurisdictions) to assign an individual transaction number to each vote. One could imagine, however, an identifying number attached to each batch of votes when votes were collected and files written. It appears to be the case that the memory card files are named only with the terminal serial number. With a batch number as well, one could then check whether that batch had already been uploaded. Mechanisms such as this might mitigate the problem of requiring election officials to assume that the process has been perfect, with no way to verify that the process has been perfect.

5.5. Software Issue: Votes Not Counted

A fault in the original software has been known to cause votes not to be counted; this fault is difficult to detect without onsite collateral information in addition to the election data.

In 2012 in Richland County, there was one terminal in each of two different precincts that resisted opening at the beginning of Election Day and was opened late by roving technicians with the technicians' PEBs. In both cases, at the end of the day, when the poll manager tried to close the terminal with the poll manager's PEB, the terminal responded with "MACHINE NOT OPENED". The two terminals had in fact been opened and had 27 and 102 votes on them, respectively, but these votes were not counted.

The error was detected entirely by chance; the first author happened to have been an observer in one of the two precincts, had taken down six serial numbers and watched all six terminals being used, and knew there was a problem when data for only five serial numbers appeared in the final record.

We remark that this is a software failure that could, and probably has, gone undetected in the past. One would not expect poll managers to collect data from terminals that declare themselves never to have been opened. We routinely see a few terminals that are not used in precincts because they are misbehaving on Election Day, so it would not be surprising to know that this has happened elsewhere and gone undetected. The only reason the first terminal was detected

was because the first author (who has the data and analysis programs) happened to be observing in one of the two precincts; even with that, the second terminal in a different precinct might not have been detected had the 2012 long-lines incident not caused a detailed look at every terminal used. The long lines triggered a legislative committee hearing and then a precinct by precinct look at terminals opened, closed, and failing, with an individual accounting for all terminals, PEBs, and memory cards used. In accounting for all the terminals and all the data, the original paper tape for the two terminals said the terminals had never been opened. It was only by going back to the warehouse and closing the terminals with a PEB (presumably with higher privileges, or with a different mechanism to force a close) that the votes were found and the files collected from the memory card.

We have not determined whether this fault still exists in the new version of the software; in order to make that determination it would have been necessary to verify the status of any terminal that had been sent to a polling place but had been reported as not being opened.

The difficulty of detecting this fault, and the importance of votes being counted, suggests the need for a strict, thorough, verification process. It is impossible to prove the absence of faults, but a regulated, controlled process would help offer some assurance in the engineering of these systems.

5.6. Software Issue: Miscounted Votes, Even With New Software

The original firmware in the South Carolina iVotronics terminals and the software of the Unity system at county headquarters was the same as that analyzed in the EVEREST report [19]. For the 2018 Primary, the counties upgraded to the central Election Reporting System version 7.7.1.0 (as is reported in the EL68A report) and to firmware version 9.2.0.2 in the terminals. The fact that we have data from both an older and a newer version of software permits an additional indirect assessment of the quality of the software.

Given the extensive documentation on the shortcomings of the original ES&S system [6, 7, 19], and our first-hand knowledge of two faults that have led di-

rectly to votes not being counted in South Carolina or to votes being counted incorrectly, we might have hoped that the known and obvious errors and problems would have been fixed in the upgraded software. Unfortunately, (at least) one fault detected earlier does persist in the new software and caused several hundred votes to be counted incorrectly.

We previously saw in 2010 in Bluffton 2C Precinct in Beaufort County that when the terminal has a different list of contests for a given precinct than are in the county's central computer, the votes from the terminal are added in based on cell location in a spreadsheet, not based on keys for the contest names. Thus in 2010, when Bluffton 2C precinct had only one of the two county council contests in its terminals, essentially all the vote counts from that point down to the bottom of the ballot were shifted up one row in a spreadsheet and added in. The end result in this case was that from that point on down to the end of the ballot, the vote counts were wrong. Constitutional Amendment 4, the last item on the ballot, received no votes for and no votes against, and in spite of the fact that 725 people voted in that precinct, this oddity was not noticed or else not considered of sufficient concern to warrant investigation by election officials or the SEC audit process.

The existence of this problem does appear in the record. In the EL68A, the line "less cands than results" indicates that there are as in Bluffton 2C fewer candidates in the terminal than in the central computer's files. The line "more cands than results" indicates the opposite, that is, that there are more candidates in the terminal than in the central computer's files for that precinct.

There should be no question that this is a software error due to two problems with the software design. First, good design would not have allowed votes to be added in without ensuring that they were added in by a key value (contest name and candidate, for example). Second, it would seem to be bad design that the ballot as stored in the terminal would differ from the ballot on the central computer. The ballot for a terminal in a precinct should be generated only once, and verified to be correct, and then copied internally if there is a need to have the ballot format both in the terminal and on the central count computer.

We would have hoped that the first design error would have been fixed. However, the same error as in Bluffton 2C in 2010 showed up in the 2018 General Election data in Bamberg's South Bamberg Precinct (Precinct 11). There were two county council districts (2 and 3) in the central computer, but only District 3 appeared in the terminal. The 420 votes for Larry Haynes (District 3) were shifted up and assigned to Sharon Hammond of District 2, and so on down the ballot. (It seems not quite that it's just moving all votes up one row, because contested races would have at least two columns for candidates and one for the write-ins, where uncontested races might only have two columns, but the effect is almost as simple as moving all votes up.)

Compounding this problem, that has led to votes being miscounted due to what must be a design error in the software, is the additional observation that the "audit" by the SEC failed to notice the problem in Bamberg County. The SEC was able in Aiken County to notice a "more cands than results" error. In that case, a referendum on alcohol sales showed up in the count of votes cast, probably from the EL155, but was not in the initial report as produced by the central computer. We thus have to assume that the SEC is aware of these errors, but it would seem that checking to verify the absence of this error is not part of the standard operating procedure. We notified Beaufort County in 2011 of their 2010 error; we have seen the error repeated elsewhere and corrected manually; and we were told that this error happened county-wide in Lancaster County in 2010 and required the county to report all votes by counting from the paper exit tapes.

The failure, however, to detect the error in Bamberg would seem to be a significant problem—even those at the SEC tasked with verifying that the results are correct seem to struggle with this task.

5.7. Software and Hardware Issues: Failure Compounding with Age

Given the lighter turnout of a primary, it was harder with the 2018 First Primary data to project terminal failures of the aging equipment. However, we

note that in the primary nearly every county had at least one terminal that failed to open properly.

In contrast to terminals that probably totally failed to function, we also observe some serious differences from one county to the next with regard to late openings of terminals. We have not seen any indication that the internal clock in the terminals actually controls anything of consequence. There is a configuration value for the poll-closing time, and if the internal clock is later than that time when a poll worker tries to open the terminal to accept one vote, an extra window pops up that essentially asks the pollworker "Are you sure?" Since voters in line at closing time are permitted to vote, the answer would normally be "yes". Other than this, however, the internal clock seems to be an entirely independent value.

This is probably a design requirement for a system like this; given the distributed nature of polling places and the requirement that Election Day be carried out regardless of complications, it would probably be a bad design decision to permit the internal clock to prevent a terminal from being used. We have seen terminals with date, month, and year set in the wrong order, terminals with the incorrect year, and even one terminal from 2010 whose internal clock was set to 12 April 2053, rolling over during Election Day to 13 April. This means that timestamp variations cannot automatically be considered to be indicators of significant problems; they could just be errors in setting the clock or a failure to reset the clock after changing out the internal battery. We note 907 of the 10,224 terminals in the 2018 General Election were nominally opened after 7:00am on 6 November. Of these, 422 were opened before 7:30am and thus might not be considered genuinely anomalous. Of greater concern would be the 250 or so terminals that were opened after 9:00am; the late open could be due to problems in opening the terminal.

We note that terminal 5135355, in Kershaw County, was cleared on 23 August, configured on 11 October, but then shows no events until it began collecting votes on *7 November 2018*—one day after the election. From the event log, we cannot tell that fraud was in process, but if this were not fraud, then it is

a significant additional indictment of the internal logging software. A similar phenomenon is observed for 5134369 and 5140418 in Darlington County, where the votes are cast on 8 November, and in 5122553 in Newberry County, with votes cast on 11 and 12 November, although at least in the case of 5134369 the time and date were reset on Election Day.

In our analysis of 2018, we have defined "Election Day events" to be events in the EL152 that occur after 7:30am on 6 November 2018. Technically, we might start the counting at 7:00am, when the polls are supposed to open, but we consider it reasonable to allow a 30-minute grace period before considering a terminal to be opened late or to be calibrated for Election Day. We note also that our definition will fail to include events that occurred on the small number of terminals whose internal clock was wrong.

5.8. Software and Hardware Issue: Timestamp Anomalies

Perhaps correlating with other event code problems, we note that the EL152 timestamps go forward and backward in time, contrary to what anyone would expect in anything that purports to be a system log. A look at the EL152 excerpt for terminal 5132179 from Chester County for the First Primary (Figure 2) says it all. Concomitant with several "UNKNOWN" events, we see the clock going back two days in time, then jumping forward and backward nine hours on the 10 June date, and then returning to what is probably the correct time and date.

We also see instances in which the timestamp is a malformed value, such as:

```
1994-01|1. -14:-26:
```

We have in the past seen timestamps that were all zeros, and we have seen some that were midnight on 1 January 1994 (this would appear to be the epochal beginning of time for the iVotronics), but we have not seen before a timestamp that did not expand properly into an actual date and time.

Another concern about the software comes from looking at the EL152 from Barnwell County. Serial number 5120526 begins Election Day with what appears to be a normal setup process. Suddenly, at 2:29pm on Election Day, the

timestamp reverts to 12 June 2018 (the day of the First Primary), and 58 votes are collected on that (alleged) date. This problem has been seen on this terminal before. In the 2014 election, the log has a "0001510 Vote cast by voter" event at 14:27:58 on 4 November and the next event is a 0001510 event at 16:30:26 on 10 June. This occurs again in 2016 with a jump from 8 November to 28 June, again with two 0001510 events, followed later by a jump from 28 June to 22 June with two 0001510 events. We find it curious and concerning that so many of these time shifts are to go back to the primary day, as if old configuration information has not been purged by the software.

Curiously, one of the five votes on this particular terminal occurs backwards in time, on 11 June:

```
        SUP   2018-06-12 07:46:15   0002900 Vote cast by voter - Visual
        SUP   2018-06-12 08:15:09   0000621 Warning: Terminal reset from voting
135993  SUP   2018-06-11 18:36:48   0002900 Vote cast by voter - Visual
136057  SUP   2018-06-12 08:22:21   0000585 UNKNOWN
135993  SUP   2018-06-11 18:44:48   0002816 Terminal-FlashFull:Vote Saved state
```

5.8.1. Hardware Issue: Screen Calibration

One of the constant complaints about the use of touchscreen voting computers is that voters touch one check box but that another box lights up. Calibration of the touchscreens is necessary to decrease the number of times this is actually a problem, and we might infer that increases in the need to calibrate screens (especially during Election Day) would be an indicator of the expected atrophy of the touchscreens themselves. For that reason, we specifically looked at the number of screen calibration events in the EL152 file.

We also note that screen calibration events seemed much more common in the 2018 elections than in the past. There were 2150 "Calibrate screen" (code 0000169) events *after* 9:00am on 12 June 2018. These would presumably not be an initial calibration for quality control purposes; those would have happened no later than the opening of the polls or one might assume no later than 7:30am. The 2150 calibration events for the primary are more than the number of code 0000169 events for the 2016 General Election and should therefore be a cause for concern.

County	2010	2012	2014	2016	2018 Primary	2018 General
Abbeville	8.62	9.80	16.33	6.67	8.33	5.26
Aiken	55.72	15.68	12.60	12.06	20.40	13.55
Allendale	16.00	30.00	17.86	18.52	0.00	10.00
Anderson	6.77	18.31	9.04	11.39	16.73	22.60
Bamberg	12.20	0.00	17.02	25.00	10.00	2.70
Barnwell	6.56	4.62	1.54	19.40	8.33	70.49
Beaufort	5.33	4.24	7.52	4.56	10.80	9.72
Berkeley	5.12	4.67	9.57	10.62	23.73	10.97
Calhoun	4.65	2.27	16.67	10.42	16.67	0.00
Charleston	3.45	8.82	8.47	8.08	9.14	5.94
Cherokee	0.75	8.51	19.29	35.71	12.64	37.10
Chester	16.09	11.58	9.38	6.06	3.75	5.43
Chesterfield	4.60	3.09	5.10	9.09	3.03	2.00
Clarendon	22.81		12.90	3.70	11.59	8.45
Colleton	3.30	6.09	6.96	2.65	2.33	7.00
Darlington	2.42	5.81	13.14	3.12	12.64	2.86
Dillon	4.11	10.84	15.49	7.35	8.70	10.29
Dorchester	12.89	14.38	11.07	14.89	14.78	8.99
Edgefield	0.00	6.35	4.29	2.90	0.00	3.03
Fairfield	0.00	2.63	1.33	2.60	2.90	0.00
Florence	4.14	4.48	2.87	8.24	6.78	3.83
Georgetown	3.57	4.94	2.56	7.32	9.02	0.65
Greenville	2.77	4.96	7.82	4.63	7.12	5.19
Greenwood	1.13	1.09	1.09	2.09	0.56	2.04
Hampton	44.62	19.72	27.94	13.43	3.08	4.76
Horry	8.99	6.39	13.64	9.41	9.62	8.47
Jasper	2.44	5.17	1.54	4.41	3.08	1.52
Kershaw	6.94	2.53	5.77	10.90	3.05	8.61
Lancaster		2.15	1.82	2.62	1.38	2.70
Laurens	3.36	11.46	5.41	2.99		3.14
Lee	1.92	6.67	7.14	0.00	0.00	12.07
Lexington	11.09	13.84	36.01	7.36	20.24	15.67
Marion	6.25	10.00	3.49	7.37	4.94	2.35
Marlboro	0.00	6.25	12.70	9.38	0.00	8.33
Mccormick	3.85	6.25	3.12	6.06	7.14	6.06
Newberry	3.19	2.08	6.19	12.00	3.23	2.08
Oconee	5.00	5.59	2.48	5.62	0.76	3.57
Orangeburg		32.68	16.26	6.07	8.82	
Pickens	2.02	1.52	3.58	2.93		2.00
Richland	10.02	13.41	10.13	27.79	24.71	38.18
Saluda	1.96	5.77	3.77	1.79	4.65	6.12
Spartanburg	1.13	1.05	2.29	3.49	4.43	3.25
Sumter	5.85	6.64	9.29	60.08	12.69	4.31
Union	21.11	1.16	3.33	14.29	10.84	6.10
Williamsburg		6.52	14.86	3.09	4.08	1.90
York	14.52	19.61	20.08	10.42	16.77	12.23
Statewide	9.27	8.88	10.60	10.83	11.83	11.44

Table 1: Percentages of county iVotronics with Screen Calibration Events, 2010-2018. Blank entries due to absence of data.

We present in Table 1 a longitudinal analysis of Election Day screen calibrations. The numbers represent the percentage of all terminals that showed a 0000169 screen calibration event on Election Day after 7:30am. For example, in the 2018 General Election, 11.44% of the 10,224 terminals in use registered a screen calibration event in this time period. We would assume that prudent county election directors would calibrate screens prior to Election Day, or at least insist they be calibrated as they are opened on Election Day, and that these events later on Election Day result from voter complaints and not the preparation of the terminals for use.

There is a huge variance in the numbers seen, with Barnwell County, Cherokee County, and Richland County clearly having calibration problems greatly in excess of the average. We have not looked into the numbers for, say, Hampton County, which started in 2010 with even higher rates of screen problems but had in 2018 a very low rate of screen problems.

The blank entries in Table 1 are from the absence of data for those elections and those counties and do not mean that there were no calibrations; if there was no EL152, we simply cannot know how many calibrations there were.

5.9. Hardware Issue: Internal Memory Issues

The iVotronic terminal has several internal memory chips and also uses an external flash memory card for saving the coded form of the EL152 and EL155 files. The cast vote record is saved in three redundant memories that are checked to be identical on an ongoing basis during use. This and other data stored or used by the terminal make use of a cyclic redundancy check (CRC) to detect garbling of the bits (and possibly also to correct some garbling). Several of the event codes, including those listed immediately below, seem to refer to memory problems. (We assume that "TF" stands for "Terminal Flash".)

```
0002202 CF -SN mismatch
0002206 Invalid index value
0002207 TF - chip vs chip crc error
```

```
0002208 Terminal flash chip compare failed
0002209 Memory block-to-block compare failed
0002303 TF - write failed
0002304 TF - operation timed out
0002306 TF - data compare mismatch
```

Of these, only the 0002209 code appears with any frequency, which is perhaps a good thing. We present in Table 2 the raw counts of the 0002209 code and in Table3 the percentages of the terminals in a given county with the 0002209 code. There have been fifteen such counties since 2010, and only two of those (Darlington and Pickens) had 0002209 events in the past but not in 2018.

The primary concern from among these error codes would clearly seem to be the 0002209 code, "Memory block-to-block compare failed". We are reasonably sure that this relates to an internal check that the three internal memories have the same cast vote record stored in them. There were 6, 2, 3, and 4 terminals that had these errors in 2010, 2012, 2014, and 2016, respectively, but 57 such terminals in the 2018 Primary and 71 in the 2018 General Election. That represents a huge change and could indicate aging equipment. If one restricts to Election Day events after 7:30am, the numbers are 0, 2, 2, 4, 25, and 49 and the dramatic increase should be alarming. Of course, it is also possible that the increase is artificial, either because the earlier software did not report all the events it should have, or because the new software has decided indeed to report them all. Each of these options would be a bad sign.

We have been concerned all along, and are now more concerned, that terminals that report hardware errors like the 0002209 code continue to be used for voting and their votes are counted as if there had been no such error event recorded. Terminal 5128090 in Georgetown County, for example, recorded 1335 instances of error code 0002209, and yet its 67 votes were collected as if no error had occurred. The 49 terminals reporting 0002209 events on Election Day reported 11,752 such events, an average of 240 per terminal; when things go

County	2010	2012	2014	2016	2018 Primary	2018 General
Abbeville	0	0	0	0	820	0
Aiken	0	0	0	0	0	1152
Anderson	0	0	0	0	80	3104
Beaufort	0	0	0	0	30	0
Berkeley	0	0	0	0	0	20
Charleston	0	0	0	0	0	20
Chester	0	0	0	0	780	0
Chesterfield	0	0	0	0	0	1652
Darlington	0	0	1	0	0	0
Dillon	0	0	0	0	40	543
Dorchester	0	0	0	0	0	920
Fairfield	0	0	0	0	0	342
Florence	0	2	0	0	0	20
Georgetown	0	0	0	0	1490	0
Greenville	0	0	0	0	440	20
Greenwood	0	0	0	0	0	1060
Hampton	0	0	0	0	0	40
Horry	0	12	25	49	0	20
Jasper	0	0	0	0	380	0
Kershaw	0	0	0	0	420	0
Lancaster		0	0	0	0	927
Lee	0	0	0	0	83	0
Lexington	0	0	0	0	1260	106
Pickens	0	0	0	6		0
Richland	0	0	0	0	0	20
Saluda	0	0	0	0	20	0
Spartanburg	0	0	0	0	20	2
Union	0	0	0	0	740	20
Williamsburg		0	0	0	20	0
York	0	0	0	0	380	1764
Statewide	0	14	26	55	7003	11752

Table 2: Counts of "0002209 Memory block-to-block compare failed" events, by county. Blank entries due to absence of data.

wrong, they seem to stay wrong, and yet there is no recourse except to ignore the warnings and count votes as usual.

We remark that we do not see the number of terminals reporting 0002209 errors concentrated in the larger counties that might expect to see a higher number of such problems. The counties with the largest numbers of these events

County	2010	2012	2014	2016	2018 Primary	2018 General
Abbeville	0.00	0.00	0.00	0.00	2.08	0.00
Aiken	0.00	0.00	0.00	0.00	0.00	2.30
Anderson	0.00	0.00	0.00	0.00	0.36	0.72
Beaufort	0.00	0.00	0.00	0.00	1.20	0.00
Berkeley	0.00	0.00	0.00	0.00	0.00	0.31
Charleston	0.00	0.00	0.00	0.00	0.00	0.13
Chester	0.00	0.00	0.00	0.00	3.75	0.00
Chesterfield	0.00	0.00	0.00	0.00	0.00	1.00
Darlington	0.00	0.00	0.57	0.00	0.00	0.00
Dillon	0.00	0.00	0.00	0.00	1.45	2.94
Dorchester	0.00	0.00	0.00	0.00	0.00	2.52
Fairfield	0.00	0.00	0.00	0.00	0.00	6.94
Florence	0.00	0.37	0.00	0.00	0.00	0.38
Georgetown	0.00	0.00	0.00	0.00	2.46	0.00
Greenville	0.00	0.00	0.00	0.00	0.27	0.11
Greenwood	0.00	0.00	0.00	0.00	0.00	2.04
Hampton	0.00	0.00	0.00	0.00	0.00	3.17
Horry	0.00	0.16	0.16	0.16	0.00	0.19
Jasper	0.00	0.00	0.00	0.00	1.54	0.00
Kershaw	0.00	0.00	0.00	0.00	0.76	0.00
Lancaster		0.00	0.00	0.00	0.00	0.54
Lee	0.00	0.00	0.00	0.00	1.85	0.00
Lexington	0.00	0.00	0.00	0.00	0.71	0.83
Pickens	0.00	0.00	0.00	1.10		0.00
Richland	0.00	0.00	0.00	0.00	0.00	0.10
Saluda	0.00	0.00	0.00	0.00	2.33	0.00
Spartanburg	0.00	0.00	0.00	0.00	0.23	0.19
Union	0.00	0.00	0.00	0.00	1.20	1.22
Williamsburg		0.00	0.00	0.00	1.02	0.00
York	0.00	0.00	0.00	0.00	0.30	0.36
Statewide	0.00	0.02	0.02	0.04	0.32	0.48

Table 3: Counts of "0002209 Memory block-to-block compare failed" events. Percentages of terminals by county with these events. Blank entries due to absence of data.

— Aiken, Dorchester, Fairfield, Lexington, and Greenwood — accounting for 30 of the 49 Election Day problems, are not the largest counties in the state. (Lexington is fourth in terms of the number of terminals used in the General Election; Aiken is ninth.)

5.10. Hardware Issue: Power and Battery Problems

We remark that anecdotal comments frequently arise with regard to battery or other power problems. Such comments were reported in 2012 regarding the incident in Richland County, for example. However, we fail to see event log records of such problems. The relevant event codes would seem to include "0001602 Terminal power is low" and "0001603 Terminal voltage read failed". We see in our data, however, only one instance of each event. If this is a problem, it is not causing events to be recorded. We remark that the only events we see that seem directly related to power issues are 0001603, "Terminal voltage read failed", reported on one terminal in the 2018 General Election, and one "0001602 Terminal power is low" event recorded for 2 July 1996 in the same election.

5.11. Hardware Issue: Undiagnosed PEB Problems

Beginning with the 2018 Primary, we have seen a problem that has been reported to stem from either a hardware or a software problem with the PEBs. In the runoff primary in Richland County on 26 June 2018, there were a number of terminals that failed to function. It was reported that some of the PEBs caused the terminals to fail either at the time they were opened or later in the election process [21]. In Williamsburg County in November 2018, there were 30 terminals that were present but not actually used, reportedly for the same problem, and we are told that this problem also occurred in Miami, Florida, in the November General Election.

The problem resurfaced during absentee voting in Richland County, and diagnosis seemed to confirm that the problem was that PEBs could and would cause the iVotronics terminals to become inoperable [21]. A rush replacement of 600 PEBs came from ES&S prior to the November Election Day, but no clear diagnosis could be made of the problem; The error messages had not been seen before either by the Richland County election officials or by staff from ES&S onsite or staff at ES&S at their headquarters in Omaha. The absentee terminals that had failed were sealed and sequestered along with two terminals that had experience similar failure on Election Day.

These terminals were to be closed by an ES&S technician, but there were four terminals in all that were not closed and whose vote data—a total of 832 absentee and 208 Election Day votes—were not included in the official count.

6. Discussion

There is no question but that elections are important; they are the primary means by which "ordinary" citizens can influence the policies of their country. Therefore, it is of crucial importance that the instruments powering elections are trustworthy. The results of our analysis suggest that this is not the case. We have observed two basic problems with the use of this electronic voting system.

The first is the inherent problem of detecting and correcting software errors when there is no way to determine ground truth of the results and virtually no way to test the software at scale except on a real event and when the software itself is viewed as proprietary and not subject to outside examination. We have seen one software error that has caused incorrect results to be produced and that has survived a revision and upgrade of the software, in spite of the fact that its occurrence is routine, having shown up somewhere in South Carolina in each of the six elections analyzed. We have seen another software error that could not be detected only by observation of the election data, since the error is an incorrect declaration that there is no data to observe. We have also seen anomalies in the output that can only come from errors in the software, but since we cannot examine the code itself and we cannot know whether other parts of the output are correct or incorrect, we are unable to determine whether these errors have led to incorrect election results.

The second basic problem we have observed lies in the fact that, as a very complicated computer system intended to be used only occasionally by volunteers, the system is incomplete in that it does not provide sufficient failsafe mechanisms to decrease the likelihood of simple mistakes. A reliance on external check lists and verification mechanisms is just not advisable given the

nature of Election Day, the number of devices to be managed, the distribution into precincts, and the rush to provide rapid results after polls close.

Even if no single error has yet caused enough damage to change the outcome of a race—*at least, in the elections we have analyzed*—each software fault arguably causes *great damage* to the users and environment of the system by falsely amplifying, misrepresenting, or disenfranchising their vote.

We take these errors as part of a major concern—even when the terminals are recording messages that indicate that the software or hardware might not be functioning properly, the votes *must be* counted from inside those terminals as if they were in fact functioning properly. To choose not to count votes from terminals with errors is to disenfranchise the voters who were directed to those terminals. However, to choose to count the votes is deliberately to include votes that might not be cast as intended.

It is a huge vulnerability in the electoral process that warnings about hardware or software failures are completely ignored, and a huge flaw in paperless DRE-based elections that when such problems occur there is no remedy. We continue to be concerned that votes are collected and counted from iVotronic terminals that declare themselves to be malfunctioning. This highlights the problem of using computers for elections when there is no means for determining ground truth and no backup capability.

A further concern is that—when issues are pointed out—the system has repeatedly been defended by attributing the mistakes to "human error" rather than flaws in the election system itself. That attribution of human error does not seem to be extended to the humans who designed and implemented the system for the vendor [1]. We do not agree with this glib dismissal of responsibility. A technology system must be designed and built to be used by the expected users under the expected conditions.

These issues raise serious concerns about the engineering of electronic voting systems. Unless usability and quality control concerns are addressed, we believe that these systems cannot and should not be trusted to manage such an important task. Traditional paper-based methods can suffer from mistakes

from human error, but the data can also be more easily validated in the case of questionable results. Traditional methods offer transparency, back-up, and verification capabilities not offered by current electronic systems.

Electronic systems *do* offer promise, and carry potential to reduce human error and waste—among other benefits. Yet, before we would suggest adoption, more must be done to improve usability and offer confidence in system quality. To that end, we would suggest that electronic voting systems be treated as the serious, safety critical systems that they are.

Software produced in safety critical domains is generally subject to strict, regulated quality control practices. For example, the DO-178C ("Software Considerations in Airborne Ststems and Equipment Certification") standard [22] is the primary set of guidelines used by the United States Federal Aviation Administration, the European Aviation Safety Agency, and Transport Canada use to certify commercial aerospace software systems [14, 20].

This standard does not guarantee software safety. No process can prove the absence of faults in a complex system. However, this standard does offer guidelines that can be used to establish a level of trust in a system. This standard requires traceability from requirement to source code, that each requirement be tested, that all lines of source code have purpose, and that system be subject to meaningful logic testing at a level of rigor appropriate to that system's level of importance. Similar standards are not imposed on the creation of electronic voting systems. We believe they should be.

However, imposing such regulation is also a difficult task. The use of airspace in the United States is regulated purely at the federal level. Therefore, the FAA is the sole authority that would need to certify an avionic system. Elections are not regulated in such a "simple" manner. What authority controls an election? The answer depends on the election in question. Some elections in the United States are federal, and there is oversight by the Federal Election Commission. Others are at the state level, and are controlled by the state authority. Others are controlled at the city level. The question of who has authority over any one election can be a contentious issue with no simple answer.

This complicates the issue of regulating the development of electronic voting systems. Nominally, the Federal Election Commission or the Election Assistance Commission (established under HAVA) could issue guidelines, but such guidelines can only by voluntary in nature. Therefore, the authorities making purchasing decisions would need to offer incentive for the corporations producing voting systems to comply with standards—i.e., make purchasing decisions based on voluntary compliance with standards and evidence of compliance.

Even the question of purchasing is complicated. In South Carolina, the current voting system was purchased by the state (with federal HAVA funds), but the individual counties are tasked with performing and paying for maintenance of these systems. In other cases, states may produce a list of acceptable voting systems, but task selection and purchasing with the counties. Therefore, imposing requirements on electronic voting systems also requires significant, complex policy decisions on the part of the authorities that will use these systems. These authorities must demand change before we can expect the quality or usability of these systems to improve. There is incentive to do so—if these systems are easier to use and offer evidence of trustworthy quality control, then the limited budgets these authorities have for managing, securing, and operating these systems will stretch further. We believe that the developers of electronic voting systems must be held to higher standards, and the responsibility for this task falls to federal, state, and local authorities.

7. Conclusion

Given the importance of electronic voting systems, such systems should be trustworthy, and their design and implementation should be held to rigorous standards. There is much that can be learned about electronic voting systems and their use by election officials by performing a critical analysis of the software quality of such systems *in the field*. In this report, we analyze eight years of election data from such systems, as used in elections in South Carolina.

Our observations include procedural errors that could be addressed through usability improvements in the systems, software quality issues—including missing log data, vote count discrepancies, multiply counted votes, ignored votes, incorrect vote tallies, and timestamp anomalies—and hardware failures—including screen calibration and timing issues, that have increased over time.

Our observations nonetheless raise multiple concerns about the software quality, hardware quality, and usability of the systems relied upon in actual elections. Given the importance of such elections, and the inherent risk in the use of current electronic voting systems, we question the wisdom of using such systems in their current form. Rather, we recommend that such systems be held to standards comparable to those used in other regulated, safety critical domains before they be trusted even on the scale that they are already deployed in the United States and other countries.

References

[1] Marci Andino. Letter from State Election Commission Executive Director Andino to the League of Women Voters of South Carolina, 01/11/19.

[2] Andrew W. Appel, Maia Ginsburg, Harri Hursti, Brian W. Kernighan, Christopher D. Richards, Gang Tan, and Penny Venetis. The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine. In *Proceedings of EVT/WOTE 2009*. Usenix/ACCURATE, 2009.

[3] Benjamin B. Bederson, Bongshin Lee, Robert M. Sherman, Paul S. Herrnson, and Richard G. Niemi. Electronic voting system usability issues. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 145–152, New York, NY, USA, 2003. ACM.

[4] Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss. DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, September 2017.

[5] Matt Blaze, Jake Braun, Harri Hursti, David Jefferson, Margaret MacAlpine, and Jeff Moss. DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure, September 2018.

[6] D. A. Buell. An Analysis of Long Lines in Richland County, South Carolina. *USENIX Journal of Election Technology and Systems*, 1:106–118, 2013.

[7] D. A. Buell, E. Hare, F. Heindel, C. Moore, and B. Zia. Auditing a DRE-based election in South Carolina. In *Proceedings of EVT/WOTE 2011*. Usenix/ACCURATE, 2011.

[8] California Secretary of State. Top to Bottom Review, 2007. `https://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/`, last accessed 24 January 2019.

[9] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *Proceedings of EVT 2007, Usenix/ACCURATE Electronic Voting Technology Workshop*. Usenix/ACCURATE, 2007.

[10] G. Gay, M. Staats, M. Whalen, and M.P.E. Heimdahl. The risks of coverage-directed test case generation. *Software Engineering, IEEE Transactions on*, PP(99), 2015.

[11] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*, pages 27–40, May 2004.

[12] Clif LeBlanc. Election data show no evidence of bias. The State (Columbia SC), 12/04/2012.

[13] Y. Meng, G. Gay, and M. Whalen. Ensuring the observability of structural test obligations. *IEEE Transactions on Software Engineering*, pages 1–1, 2018. Available at `http://greggay.com/pdf/18omcdc.pdf`.

[14] Y. Moy, E. Ledinot, H. Delseny, V. Wiels, and B. Monate. Testing or formal verification: Do-178c alternatives and industrial experience. *IEEE Software*, 30(3):50–57, May 2013.

[15] Anitha Murugesan, Sanjai Rayadurgam, and Mats Heimdahl. Using models to address challenges in specifying requirements for medical cyber-physical systems. In *Fourth workshop on Medical Cyber-Physical Systems*, April 2013.

[16] Clark S. Turner Nancy G. Leveson. An investigation of the therac-25 accidents. *IEEE Computer*, 1993.

[17] United States Government Accounting Office. GAO, Elections: Further Testing Could Provide Increased but Not Absolute Assurance That Voting Systems Did Not Cause Undervotes in Florida's 13th Congressional District, 10/02/2007. GAO-08-97T.

[18] United States Government Accounting Office. GAO, Elections: Results of GAO's Testing of Voting Systems Used in Sarasota County in Florida's 13th Congressional District, 2/08/2008. GAO-08-425T.

[19] Ohio Secretary of State. EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing, December 2007. `https://www.eac.gov/documents/2017/03/21/everest-report-state-voting-systems-voting-tech` last accessed 31 December 2018.

[20] Lianna Rierson. *Developing Safety-Critical Software*. CRC Press, Boca Raton, FL, USA, 2013.

[21] Rokey W. Suleman. Memo to the Richland County Board of Registration and Elections. 10 February 2019.

[22] RTCA/DO-178C. Software considerations in airborne systems and equipment certification.

[23] Ian Sommerville. *Software Engineering*. Addison-Wesley Publishing Company, USA, 9th edition, 2010.

[24] South Carolina State Election Commission. Canvass Checklist, SEC FRM 1099-201010. Obtained by FOIA.

[25] South Carolina State Election Commission. Election Audits. `https://www.scvotes.org/election-audits-south-carolina`, last accessed 31 December 2018.

[26] South Carolina State Election Commission. Website. `http://www.scvotes.org`, last accessed 31 December 2018.

[27] Verified Voting. Website. `http://www.verifiedvoting.org/verifier`, last accessed 5 February 2019.

[28] Chris Whitmire. Letter from SCSEC to Duncan Buell in response to a FOIA request, 12/17/2010.

[29] Alec Yasinsac, David Wagner, Matt, Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos, and Mike Burmester. Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, 2/23/2007.