DEPARTMENT OF INFORMATION RESOURCES

P.O. Box 13564 ◆ Austin, TX 78711-3564 ◆ www.dir.state.tx.us
Tel: (512) 475-4700 ◆ Fax: (512) 475-4759

February 4, 2005

Ms. Ann McGeehan
Deputy Assistant
Office of the Secretary of State
1019 Brazos Street
Austin, TX 78701

RE: Examination of the Unity Election System Version Release 2.4.3 and Vote Tabulation Devices from Election Systems and Software (ES&S)

Dear Ms. McGeehan:

I attended a scheduled examination January 6, 2005, at 8:30 am, for the purpose of examining updated modules of the voting systems from ES&S and for certifying a new product, AutoMARK. The report below summarizes my findings.

Hardware/Software Version

Unity Election System v2.4.3, last certified January 2004
The updated modules that were examined include the following:
Hardware Programming Manager v5.0.3.0c
Data Acquisition Manager v5.0.3.1b
Election Reporting Manager v6.4.3.0a

Hardware
Model 150/550 Central Countv2.1.1.0a

DRE voting systems
iVotronic Direct Recording Electronic (DRE) voting system v8.0.1.0r
PEB 1.07

Issues from previous examinations

Because the ES&S product line is significantly more complex than other vendors in the industry, some of the issues surrounding their products require more in-depth explanation than is generally given in this report. Thus the background, analysis and detail findings for Real-time log printer on the Data Acquisition Manager, resetting voting terminals to zero, and the printing zero total tapes issues summarized below are provided in Appendix A, attached.

Issue: Real-time log printer on the Data Acquisition Manager (DAM)

This examiner finds no convincing reason to require a real-time log printer either at the clients in the regional sites or on the server at election central. However, it is recommended that all events logged at the DAM clients be transmitted to the DAM server and consolidated in the ERM.

Issue: Resetting voting terminals to zero when polls are opened

This examiner finds that the ES&S architecture and design philosophy supports their recommended operating procedures. The voting anomalies observed during a prior examination are most likely an artifact of the examination process rather than significant threat to the integrity of the voting system.

Issue: Printing zero total tapes

This examiner finds that the system architecture also dictates the procedures the vendor recommends for printing zero tapes when opening the polls. As such the current procedures appear to be adequate although not ideal. It is suggested that the vendor modify the internal programming of the PEB so that no further administrative actions can be taken until a zero tape has been printed. This ensures that a zero totals tape will be printed before the polls are closed.

Issue: Real-time log printer on the Election Reporting Manager

The vendor demonstrated that the real-time log printer functions as current SOS rules require.

Issue: Model 150/550 disk read errors
The vendor discussed problems with reading disks produced by the 150/550 counters. Apparently a small bug in the software caused intermittent read errors. The vendor claims to have fixed the error and the system as demonstrated now appears to work as advertised.

Issue: Duplicate disk read error reports
The software now appears to log all disk reads, including attempts to read a disk more than once. It is strongly suggested that such errors also be reported to the operator on screen. This might save some time and potential embarrassment since duplicate disk reads might look like attempted fraud.

Recommendations

DIR finds no technical objections to certifying all of the system components presented at this examination.

AutoMARK certification

System Description

AutoMARK is described as a "Voter Assist Terminal" (VAT), an interface between a paper ballot and the voter. The device reads the ID codes on an optical scan ballot, determines what races and initiatives should be voted, provides several methods of making the ballot accessible to users, and several methods for the user to vote. It also marks the ballots with the user's choices.

In effect, AutoMARK is a highly sophisticated "pen" that reads and marks ballots for the disabled. It does not tabulate votes, but only produced an optical scan ballot marked with the user's choices. This allows jurisdictions to keep their current optical scan equipment and voting processes, but still comply with HAVA requirements to provide voting accessibility devices at every polling location.

System components and operation

AutoMARK is a stand-alone device that is portable enough that it can be carried to a

voter at curbside. It has a scanner with which to read ballots, a printer with which to mark them, and an internal computer in which it stores ballot definitions. Ballot definitions can be downloaded from several vendors' ballot definition software so the equipment is not limited to using ES&S ballot styles. The system software can read all current optical scan ballots in several sizes and interpret the timing marks to determine where to mark the ballots based on the ballot definitions.

The device has a touch screen that can be used to select choices, as well as a touch pad, and a puff-sip tube for users who cannot use the touch screen or touch pad. The system also allows the user to enlarge print on the touch screen for users with limited vision, and includes voice synthesis software that can provide audio of ballots in several languages common in the U.S.

The voter simply feeds the ballot into the slot in the front of the machine. The software then determines which ballot it is and presents the ballot choices to the voter. Voters who use the audio ballot through a headset can blank the screen so their choices cannot be seen. The unit provides a summary screen and/or an audio summary of the choices before asking the voter to cast the vote.

The software prevents overvotes and warns the user of any undervotes. When the voter casts the ballot, the unit's printer fills in the proper ovals or connects the correct arrows and returns the marked ballot to the voter. At this point the ballot can be handled as any other manually marked ballot.

Findings

The system as examined marked ballots correctly and performed as any other DRE device. The only difference is that it produces a marked paper ballot rather than recording votes electronically. Since the system is not a tabulation device, it does not need a real-time log printer.

Recommendation

DIR finds no technical objection to certifying AutoMARK as a standalone voter assist device.

Respectfully,

Nick Osborn
Systems Analyst

Appendix A
Analysis of Issues from Prior Examinations

Data Acquisition Manger (DAM) Issues

System Description

Purpose of DAM

The Data Acquisition Manager (DAM) is an intermediary system that collects vote tallies from voting locations and transmits them to election central electronically. This approach enables much faster tabulation of votes and reduces congestion at election central. This is particularly important for large jurisdictions.

System components

The DAM has two components, a client and a server. The server is a single computer located at election central that collects vote tallies from DAM clients via modem. DAM clients are computers located in remote locations within the voting jurisdiction (ES&S calls these "regional sites"). Thus a jurisdiction would have one DAM server and multiple clients at strategic locations as shown in Figure 1 below.

On election night the DAM server connects to the DAM remote sites through dialup phone lines. Once established, the connection is continuous unless the phone service is disrupted or until the connection is terminated by either the client or the server.

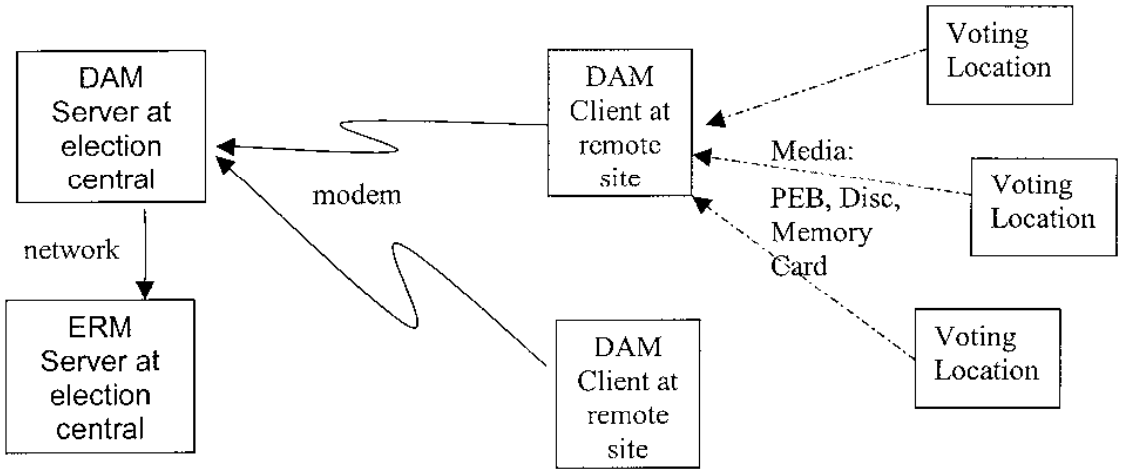

Figure 1 Schematic of DAM clients, DAM server, and ERM server

The DAM clients communicate with the DAM server using a proprietary protocol, and includes passwords that can be changed for every election. Voting data is transferred through proprietary protocols, the data structures are proprietary and the data itself is

unreadable without knowledge of this proprietary protocol and a separate election definition map that is different from election to election.

There is no direct communications between DAM and the Election Reporting Manager (ERM). DAM will simply place election results data vote tally files on a secured, but shared directory on a closed, secured Local Area Network (LAN) file server that ERM also has access rights to. When in "accumulation" mode, ERM continuously looks for new files on the shared LAN server directory. When such files show up, ERM will process and accumulate such results vote tallies, adding them to the ERM results reporting database. The ERM logs all such actions on the real-time log printer and real-time electronic logs.

System Operation

When the polls close, poll workers tally votes from paper ballots or voting devices. The vote totals are copied onto media such as PEBs, disks, or memory cards. The workers then bring the media to the DAM client sites. The DAM client software reads the tallies from the media and stores them on its local hard drive.

On a continuous basis, the DAM server at election central contacts each DAM client and downloads any new tallies in the DAM client into the secured LAN server directory shared by ERM, for subsequent processing by ERM as described above.

Real-time Audit Log Issues

Texas requires electronic tally systems to log all activities that may affect recording, tallying, and reporting votes. In the past this has been interpreted to include actions such as downloading vote totals from transfer media such as memory cards to the central count system.

The DAM is an intermediary system. It does not change any data, but merely transfers vote totals accumulated from the voting locations to the central count location. While the DAM does not change any data, the process of transferring vote data from the voting location sites to the DAM client does provide a slight opportunity to insert forged data into the data transfer process. This vulnerability, though admittedly small, seems to be a valid reason to require data exchanges at the DAM to be logged. ES&S confirms that the DAM clients and server do log such actions.

Note that the data files are transferred through DAM in a proprietary format through a proprietary protocol and are protected by checksums and/or other authentication codes. It is not a trivial task to forge a vote tally that the ERM will accept. The likelihood that the vote tallying system will be compromised successfully through the DAM is low, perhaps bordering on negligible.

Thus the main benefit of logging all data transfer actions seems to be forensic—to establish if and when any unauthorized attempts were made to add fraudulent data to the system. The key question then becomes whether the benefits of having a real-time log printer at each DAM client outweigh the potential liabilities. Key liabilities include increasing the number of failure points such as a malfunctioning printer, and requiring additional training of personnel at the DAM client sites.

The purpose of the log printer at Central Count is to discourage tampering with the vote tallying process. Under current procedures the system cannot be operated if the log printer is not online to record every significant transaction. Thus an operator cannot use the vote tally system to change vote totals covertly. The effect is more cosmetic than real, however. All transactions through the ERM are logged electronically even if they are not printed in real time. The printer just serves as an audible, visible reminder to the operators that their actions are being logged.

Applying the same procedure at the DAM client may not provide the same deterrent. The DAM client software cannot be used to change data in any files in the way that the ERM software can. Tampering with the data would have to occur beforehand by an individual creating a forged file. The forger would bring in a data file and attempt to have the DAM client read and accept the forgery. If the file is not read successfully, the client software reports it to the operator by a message on the monitor, a response that is likely to be more effective than printing out the report on a printer. Thus it would seem that the current security processes are probably more effective than an additional log printer would be.

Recommendations

1. This examiner cannot find a compelling reason to require a real-time log printer at DAM clients.
2. If changes are made to the logging procedures, it seems far more important to insist that all activity logs be consolidated into a single database. Every activity within and among all components of a voting system should be easily available for forensic examination, and open to the public. Such transparency would go a long way to discouraging attempts to compromise the voting systems. It would also increase the likelihood that any such attempts will be discovered.

   With that goal in mind, it is strongly suggested that the DAM client logs be downloaded to the DAM server at the same time the data is transferred. It should be consolidated by the ERM into a single election activity log. Further, it is suggested that any logs in media such as PEBs, memory cards, and disks also be downloaded through the DAM to the ERM.
3. It is recommended that the vendor develop log inspection software that enables the user to sort, view, and analyze all logged activities of all components of the system from opening the polls to producing the final election results.

Zero Totals Issues

Design Philosophy

The iVotronic architecture is described by ES&S as "closed" and non-networked. Each Direct Record Electronic (DRE) voting device is a standalone unit with its own internal non-volatile memory, computer, touch screen, power supply and battery backup. Each iVotronic has a unique internal serial number. This architecture eliminates the possibility of widespread breakdown that might occur with networked devices.

However, because the devices are standalone, certain administrative functions such as preparing machines for voting must be done one machine at a time. In addition the vendor provides fine-grained administrative functions that can also be applied one machine at a time by personnel with appropriate administrative passwords.

This approach provides considerable flexibility to election administrators. For instance, they can easily add additional voting machines to a voting location without disturbing voters who are voting on existing DREs at the location. This flexibility comes at the price of additional complexity, however. Such flexibility must be managed by a disciplined elections administration that follows procedures rigorously.

System Description

System Design

Because the DREs are standalone units; they cannot be programmed *en masse* through a network. Instead, they are programmed and activated individually through a unit the vendor calls a Personal Electronic Ballot (PEB). The PEB is a handheld cartridge with its own nonvolatile memory and computer that is inserted into a special slot in the DRE. The PEB communicates with the DRE through an infrared port, eliminating the possibility that the units can be subverted through unauthorized electronic access.

The PEB and administrative passwords give the poll workers operational access to each DRE. Poll workers use the PEBs to

- Load election definitions into each DRE prior to opening the polls and print zero total tapes,
- Select the ballot style and enable (unlock) the DRE for each voter to use,
- Close the polls at each DRE, tally votes on the DRE, and print the tallies
- Transport the vote tallies to the Central Count location.

Since a PEB must be used to activate a DRE for voting and select the ballot style each time a voter uses the DRE, a polling location will usually have more than one PEB. However, only one of the PEBs is the designated Master unit used to prepare the DREs when the polls open and to close the DREs and tally votes when the polls close. The Master PEB will log all the DREs it has opened for voting, the time they were opened, and other key events. When the polls are closed, the Master PEB is used to close the voting machines in the precinct.

As a failsafe contingency, in the event the Master PEB that was used to open terminals at the start of the day, sometime later fails, a second PEB (backup) can take over the role of the Master PEB, and allow the end of night terminal closing process and vote results collection process to continue. If this failsafe contingency process is used, the second Master PEB (backup) event log will reflect such activity.

System Operation

The table below is a simplified chronology of the process recommended by the vendor for managing voting devices for an election.

Stage	Election Definitions and PEBs	Ballots and DREs

Stage	Election Definitions and PEBs	Ballots and DREs
Pre-Election	Election definitions are created in the vendor's ballot creation software at election central.	
Clear and Test	Election definitions are downloaded into PEBs at election central, and "Clear and Test" PEBs are created to prepare the voting devices for the new election. Supervisor PEBs are created for each voting location. A supervisor PEB for a specific polling place contains only the ballot styles allowed at that polling place.	At the warehouse where the DREs are stored, "Clear and Test" PEBs are used to erase election definitions and votes from the prior election from the DREs. Test ballots are voted, test results are documented, test votes are cleared from the machines. Note that the firmware will not allow the machines to be opened for voting until test votes have been erased.
Distribution	PEBs are distributed to poll workers who take them to polling locations.	Warehouse personnel distribute DREs to the voting locations.
Opening Polls	At the polling locations, poll workers • Designate one PEB as the Master PEB. • Insert the Master PEB into each of the DREs to download the ballot styles for that polling location, and open the machines for voting. Note that if any DREs have been left in testing mode or have votes already on them, the Master PEB cannot open them for additional voting. They must be cleared and re-opened using a special administrative password. • Use activator (non-master) PEBs to activate each voting machine and select the proper ballot style for individual voters. Alternatively, they may provide voter PEBs that allow voters themselves to activate the voting machines.	
Closing Polls	Poll workers close the DREs with the Master PEB, tally votes, and print the vote total tape. They take the Master PEBs to a regional count or central count location for tallying votes.	Warehouse personnel pick up DREs and return them to the warehouse. Any election definitions and votes stored on an iVotronic remain in non-volatile memory until they are deleted by an operator with an administrative password

Clearing votes on DREs

In the chronological scenario above, the units are reset to zero, and Logic and Accuracy (L&A) tests are done before the devices leave the warehouse. Any machine that arrives at a polling location with votes still on it cannot be reset to zero by poll workers because

they do not have high-level administrator passwords. A machine that has votes on it indicates either mishandling at the Clear and Test stage, or potential vote fraud.

Mishandling can include occurrences such as taking a DRE that has been used for early voting to a precinct for election day voting. If votes are not collected from such machines before moving them to precincts, clearing the machine would lose all votes that had been cast during early voting. The system as currently designed prevents this from happening accidentally. While a DRE can be opened early and votes can be cast on it, the machine cannot be closed and then reopened again without administrative intervention. All such administrative actions are logged and the records can be retrieved for audit.

Printing the zero tape

Because of the system architecture and operating philosophy, the Master PEB does not know how many DREs to expect at the polling location. It cannot know when to print a zero tape; the poll worker who opens the machines must print a zero tape when the last DRE is opened.

Thus the polls *can* be opened without printing a zero tape, however to do so, the election administrator would have chosen to *not* print the zero tape when queried by the system, overriding to protect votes that should not be removed from the DRE. The master PEB, however, does retain a record of all DRE vote totals at opening, and a log of all actions that were taken when the devices were opened.

Vote anomalies at a prior examination

The vendor's procedures for clearing the voting devices is consistent with the system's design philosophy. Further, it appears that their rationale for not providing a function to clear the machines as the polls are opened is also reasonable, given such design principles. However, this also requires that the system be managed by a disciplined elections administration that follows procedures rigorously.

The question still remains, how did the voting anomaly in a prior examination occur? As the vendor has noted, the examination environment is considerably more complex than a typical jurisdiction would be, even a large one. For instance, at a typical exam the vendor brings nearly all of the hardware and software they produce in order to simulate numerous voting configurations that different jurisdictions may have. However, no jurisdiction will have such a wide variety of hardware and software.

In addition, the vendor brings along highly skilled personnel who reconfigure equipment and software on the fly to help examiners explore system operations and options. Apparently it was this aspect of the examination environment that caused the anomaly. It seems that votes were left on one of the units that the vendors' technicians had been using to answer examiner's questions. The votes were added to the totals in a subsequent voting test and give the impression that the security of the system had been compromised. In that regard, the examination was not so much a test of how the system might be used as much as a reflection of the *ad hoc* nature of the examination itself.

It is highly unlikely that a jurisdiction would have such a wide variety of hardware and software. It is even less likely that they would have highly trained personnel making numerous capricious changes to system configurations. Finally it is a still more remote

probability that it all this would be occurring during an election. On the contrary, a well-controlled elections jurisdiction will attempt to simplify and standardize all aspects of elections to make them manageable and auditable.

Recommendations

1. During an examination, it is fruitful to have highly skilled personnel who can reconfigure equipment at the drop of a suggestion. This enables examiners to probe potential system vulnerabilities more easily. However, to simulate real-world conditions at these examinations, it is suggested that end-to-end system tests be more tightly controlled for each potential configuration that is examined. This approach will more accurately reflect how a jurisdiction might use the system.
2. Given the initial design philosophy, it appears that the vendor has provided adequate procedures and safeguards against vote tampering. Thus the recommended processes for clearing and testing the machines prior to opening the polls seem to be reasonable.
3. It is recommended that the vendor provide some safeguard to ensure that zero tapes are printed at some point. This might be achieved by having the Master PEB refuse to perform any administrative functions such as closing the polls until it prints zero tapes. Such a tape might be printed much later than at poll opening, but the print time would be indicated on the tape, and would be logged in the PEB.
4. To reiterate, it seems highly important to insist that activity logs of all devices be consolidated into a single database at election central. Every activity within and among all components of a voting system should be easily available for forensic examination, and open to the public. Such transparency would go a long way to discouraging attempts to compromise the voting systems. It would also increase the likelihood that any such attempts will be discovered.