Mr. John Mott-Smith 2 Sep 2004
Director of Voting Systems
Office of the Secretary of State
1500 11th Street
Subject: Certification of Election Systems & Software (ES&S)'s
Unity 2.4.3 Election Management System (limited to AM, EDM, ESSIM, HPM, & ERM)
M100 Precinct Ballot Counter (Rel 5.0.0.0)
M550 Central Ballot Counter (Rel 2.1.1.0), and
M650 Central Ballot Counter (Rel 1.2.0.0),

Executive Summary

State certification testing was conducted 14-17 June 2004, in Omaha, Nebraska, to certify the Election Systems & Software (ES&S) Unity 2.4.2 package with the Model 100 and M650 Ballot Counters. Difficulties with the California Primary election features were discovered and the system was withdrawn for further work and testing. Testing resumed in Sacramento 19-22 Aug 2004 with a revised Unity 2.4.3, the unchanged M100 and M650, and the addition of the new 2.1.1.0 release of the M550 Central Ballot Counter.

The iVotronics, the Optech IV-C, the Optech Eagle III-P and related Unity modules were not tested or reviewed for certification.

Review and testing of this proposed configuration showed compliance with the California Election Code. There are some serious concerns over security access issues. One possible action may require additional software security review, pending the results reported in the final Federal ITA report which is pending.

References:

1. [Cal2004], California Legislature, *California Election Code*, Jan 2004
2. [M650] Wyle Report# 48489-03, *Change Release Report of the ESS Model 650 Mark-Sense Central Ballot Counter (Firmware Release 1.2.0.0),* 24 Feb 04.
3. [M100] Wyle Report# 48489-03, *Change Release Report of the ESS Model 100 Precinct Counter (Firmware Release 5.0.0.0)*, 25 Feb 04.
4. [M550] Wyle Letter# 48489B-22, *ITA Hardware Qualification Testing of the ESS Model 150/550 Central Ballot Counter, Firmware Release 2.1.1.0, 18* Aug 04.
5. [Unity] Ciber Letter, *Status of Unity 2.4.3,* 28 July 04.
6. [Unity2] Ciber Report, *Election Systems and Software International (ES&S) Software Qualification Test Report, Amendment 2, Unity 2.4.3 Updates for 1990*, 27 Aug 04

Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following revisions:

1. ES&S, Unity 2.4.3,
   a. Audit Manager (AM) v. 7.0.2.0
   b. ES&S Ballot Image Manager (ESSIM) v. 7.2.0.0
   c. Election Data Manager (EDM) v. 7.2.1.0
   d. Hardware Programming Manager (HPM) v. 5.0.3.0
   e. Election Reporting Manager (ERM) v. 6.4.3.0
2. ES&S, M100 Precinct Ballot Counter, Firmware Ver. 5.0.0.0
3. ES&S, M550 Central Ballot Counter, Firmware Ver 2.1.1.0
4. ES&S, M650 Central Ballot Counter, Firmware Ver 1.2.0.0

(Attachment A has equipment specifications for the Test Configuration)

Unity is a suite of integrated programs which can be installed to support the specific ballot counters needed by the election jurisdiction. The tested configuration was for three of the optical scanners but excluded:

a. the Model 150 Central Counter,
b. the iVotronic Touch Screen DRE Voting System
c. the Votronic
d. the Optech III-P Eagle Precinct Counter,
e. the Optech IV-C Central Counter
f. the following Unity 2.4.3 modules
    i. Data Acquisition Manager (DAM)
    ii. iVotronics Ballot Image Manager (IM),
    iii. Optech Image Manager (OIM)
    iv. Ballot On Line (BOL)

Significant Change

The Unity version releases since 2.4 have largely been adding ballot counting devices to the list of approved devices and bringing the suite of programs and equipment under the Voting Systems Standards for 2002. The Unity 2.4.3

- added M100, M550, and M650
- support the California primary under Sections 13102 and 15151 of the California Election Code
- support larger elections/ballots
- adding absentee ballots cast to the California Statement of Vote header
- correction for problem detected in earlier testing of Unity 2.4.2.

M100 changes include:

- support for the larger elections
- added/re-installed features of the ES&S calibration reports
- better detection of various ballot problems including counterfeit ballots
- improved handling of two sided ballots
- updated system readiness report including battery check

M550 changes include:

- allow more ballot styles per precinct.

M650 changes include:

- allow more ballot styles per precinct
- support California primary.

Qualifications

NASED Qualification

1. N-1-02-12-11-001 (1990), 19 Feb 2004 includes:
    a. Unity 2.4.2
        i. Election Data Manager v. 7.2.1.0
        ii. Audit Manager v.7.0.2.0,
        iii. ESS Image Manager 7.2.0.0.
        iv. Hardware Programming Manager v. 5.0.2.0,
        v. Election Reporting Manager v. 6.4.2.0
    b. Model 100 Optical Scan Precinct Ballot Counter Firmware v. 5.0.0.0
    c. Model 150/550 v. 2.1.0.0 M
    d. Model 650 v. 1.2.0.0
2. Final ITA Qualification Test Reports have been produced and are in final review by the NASED Voting Systems Board Technical Committee prior to release of a NASED Qualification number.

Test Results

The test election was based on the San Diego 2002 Primary and General with the addition of Presidential race (with semi-fictional candidates to complete General election) in seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing DTS voter participation and reporting with the Republican DTS not permitting participation in Presidential nominations (See details in Attachment B). During the earlier Unity 2.4.2, correct counts were provided by the M100 and M650 but a problem was discovered in the data uploaded from those counters in the Unity 2.4.2 reporting. ES&S corrected the problem and resubmitted the changes to the Federal test laboratories for NASED qualification. The condition was recreated for the Unity 2.4.3 state certification testing and all results were reported correctly.

Security Controls

Unity is collection of mixed programs. The design and access controls on the Election Data Manager (EDM) use different standards, programming languages, audit log controls, and databases than the Hardware Programming Manager (HPM) or the Election Reporting Manager (ERM). (See the Observation section of Appendix A for details) The access methods for the different units default to disabling the access controls to be disabled or not initializing them at the start. When used, the design supports separation of function and software security principles involving implementing the least privilege needed to perform the task. ES&S procedures, however, tend to emphasize the use of restricted physical access to the equipment as the main security control required. Although physical access is a valid control, for effective logging and other reasons, the available user ID and/or password controls should actively be used in Unity.

The paper ballots themselves are a major security element. The election definition can be rebuilt in HPM based on a full sample set of the ballots and the election results can be replaced by the rescanning of the saved ballots. Ultimately, the integrity and security of the election is limited/supported by the secure handling and storing of the ballots themselves.

Unity is currently not compatible with Windows XP, Service Pack 2 under the default installation.

[redacted]

Conclusion

Review and testing of this proposed configuration showed compliance with the California Election Code. There are some typical concerns over security issues where current practices are overly dependent on active restricted physical access but procedures involving removing key components for overnight storage and active use of available access controls in Unity and the underlying operating system are viable.

Sincerely,

Steven V. Freeman

Steven V. Freeman

Two Attachments:

A. Hardware Description with a list of the test configuration components.
B. Test Election Design

Attachment A.

Hardware Descriptions

Model 100 Precinct Ballot Counter (Ref. Model 100 Specifications)

The Model 100 (M100) Precinct Ballot Counter mounted on Ballot Box. See detailed Specification sheet for more details. The M100 is based on the QNX 4.22 operating system and uses an Intel 286EX Processor. The optical sensor is sensitive in the visual light spectrum and detects changes in marking across the page as the ballot passes under the scan head. The device is programmed to recognize ballots common to the M150/550/650 line of ballot scanners and can take the ballots in any orientation.

The M100 uses PCMCIA 512K/2M Memory Cards to install the election definition and to store/transfer the election results after polls close. The PCMCIA card is secured during the election with a front panel/cover with a seal point for wire security seals or lock.

The M100 has two RS232 ports. The ports are not used during election day and may be secured with a metal cover like the PCMCIA slot cover.

Model 550 Central Ballot Counter

The Model 550 (M550) Central Ballot Counter with the two printers connected. The M550 is an optical mark sense scanner but uses a different technology than the M100. . The M550 uses a proprietary controller program rather than an operating system and is based on a Z80 processor. The scan head uses fixed position sensors for the front and back of the ballot and supports 1-3 columns on the front and back of the ballot. See the detailed Specification sheet for more details

The election program is installed in a removable EPROM which can be secured in a safe location until needed. The RAM is volatile and does not retain the vote count results when power is lost. Procedures require periodic checkpoint/recovery saves to a 3.5 diskettes until the election is completed. The diskettes are used to transfer and store the results to an accumulation device such as another M550 or Unity server with Election Reporting Manager installed.

Model 650 Central Ballot Counter

The Model 650 (M650) Central Ballot Counter with the two printers connected. The M650 uses the similar optical mark sensor design as the M550 but has a straight through ballot feed path to a receiver bin to the side. The M650 is a faster counter than the M150 or M550. See the detailed Specification sheet for more details. The M650 is based on QNX 4.25 operating system.

The M650 has an internal solid state hard drive and can retain election results if power is lost but the operator must save the results periodically to the hard-drive. Results are not stored

automatically. The M650 uses 100MByte Zip disks to install the election definition to the hard-drive and to save, transfer, and restore results to another scanner or Unity ERM module.

The M150 (not submitted for certification), M550, and M650 support two continuous feed hardcopy printers: one serves as a log and the other serves as a report printer. Should one of the printers become disabled, its printing role is switched automatically to the other printer. All versions will support operations on a single printer.

Test Configuration

1. Unity Server
    a. Model and Serial Number: Dell D600 Latitude laptop, Dell #: C5MFW41
    b. Processor: Intel Pentium M 1.7GHz
    c. Memory: 1024 Mbytes installed
    d. Operating System: Windows XP, Service Pk 1
    e. Hard Drive: 30 GBytes
    f. Other drives:
        i. Removable 3.5 Diskette Drive module
        ii. Removable CD-R/DVD Drive module
        iii. Iomega 250 Zip Drive (USB)
        iv. Omni Pro, PCMCIA Card Reader/Writer
        v. EMP-11 EEProm burner (modified to use a Bakelisht carrier).
    g. Printer: HP 4100
    h. Display: Laptop
    i. Keyboard: Laptop
    j. Mouse: ATI Touchpad/optional bus mouse
    k. Communication Ports:
        i. Internal Modem. Not used for testing
        ii. Ethernet port. Not used for testing.
    l. COTS Software:
        i. Crystal Reports 9.0
        ii. Codebase 6.5, revision 3 (MDAO compatible database)
        iii. Adpbe Acr\obat Standard 5.0.5 with special Helvitica font
        iv. MS Access (for Audit Manager)
        v. RMCobol 7.50.01,
        vi. COBOL WOW 3.12,
        vii. OmniDrive driver version 2.21 (standard drive),
        viii. USB Drive version 1.72
        ix. Iomega Zip Disk (USB-250MB) ver 3.2.1.5
        x. Java 2, Rel 1.4.2_3 (this is an older version than what was initially installed on the server)
        xi. Omni Driver

2. Voting Unit(s)
    a. Model and Serial Number: M100
    b. Model and Serial Number: M550
    c. Model and Serial Number: M650

Observations:

1. No definition or recommendations for securing the Windows environment is provided by the vendor. ES&S recommends isolation of the Unity servers with no telecommunications or other uses ould expose the servers to virus or other forms of attack.

2. The design of Unity is a mix of different programming environments and databases. The election definition and ballot layout modules use a DAO (MS Access type) database for maintaining access controls as well as the election definition itself. The hardware programming and election reporting modules use COBOL and indexed sequential databases.
   a. Controls on Audit Manager (AM) (MS Access type database)
      i. [redacted]
      ii. [redacted]
      iii. [redacted]
      iv. [redacted]
      v. [redacted]
      vi. [redacted]
      vii. [redacted]
      viii. [redacted]
   b. . Login ontrols on HPM (COBOL indexed sequential database)
      i. [redacted]
      ii. [redacted]
      iii. [redacted]
      iv. [redacted]
      v. [redacted]
      vi. [redacted]
      vii. [redacted]
      viii. [redacted]
   c. Login controls on ERM (COBOL indexed sequential database).
      [redacted]
      i. [redacted]
      ii. [redacted]

3. Hidden utilities.

   The HPM and ERM applications are written in COBOL with a runtime engine installed as RMCOBOL. The COBOL executable files may be set up to run with options on a command line but user documentation is not provided. As COBOL programs, the programs may include methods to open, access, and change the database. The limited testing time and other problems in testing did not permit time to investigate what could be done.

4. Additional executable modules/files.

   [redacted]

   i. [redacted]
   ii. [redacted]
   iii. [redacted]
   iv. [redacted]

v. [redacted]
vi. [redacted]
vii. [redacted]
viii. [redacted]
ix. [redacted]
x. [redacted]
xi. [redacted]
xii. [redacted]

5. The M100, M550, and M650 designs use keyed locks. The default key is not unique but the key cylinders may be replaced with uniquely keyed locks. Tamper-proof seals may be needed, if the keys are not replaced when the programs are installed but the programs are easily removed and stored in more secure storage such as a safe or secure vault when the units are not active.

6. Marginal Marks/calibration
   a. Mark sense systems which depend on human voters marking the ballot with ink or pencil are vulnerable to marks which are not clearly valid (such as a filled in oval) or not countable (a dot created where the voter tapped the pencil against the ballot target area). The class of marks between the always accepted and always ignored are sometimes called "marginal marks' and have the undesirable feature of not always being counted the same way (equivalent to hanging chad). Most of the optical scan systems in use today have very low incidences of marginal marks and a common situation is for the variation due to marginal marks to be less than the human error in manual recounts of paper ballots.
   b. The ES&S optical mark reader ballot scanners have two features that work to take positive control of the marginal mark problem. With this change, the scanners will halt on ballots with marginal marks and require resolution. A calibration report is available that will show which marks are positive, which are below acceptance standards, and which require human review to determine voter intent (is the marginal mark consistent with the way the voter marked other races?).
   c. The calibration report was originally designed as a technician tool to check the performance and sensitivity of the sensors. This feature still serves that purpose by giving an early warning of deterioration of a sensor requiring adjustment or other servicing.

7. Duplicate names. The EDM module accepts duplicate names between races. A duplicate name may be valid but usually is an error needing detection and correction. Must be caught as part of manual proof reading.

8. HPM is designed to permit coding of the election directly from printed ballots rather and does not need to download a definition from the EDM.

9. Rotation. First contest requiring rotation was automatically created with the correct rotation. Subsequent races needed to be adjusted manually.

Attachment B.

Test Election Design

	Precinct	1	2	2	3	4	5	6	7	8	9	10
Type	Split		1	2								
SW	Federal, STATE	x	x	x	x	x	x	x	x	x	x	x
SD	Board of Equal 3	x	x	x	x	x	x	x	x	x	x	x
SD	CONGRESS 49	x	x	x								
SD	CONGRESS 50				x	x						
SD	CONGRESS 51						x	x				
SD	CONGRESS 52								x	x		
SD	CONGRESS 53										x	x
SD	STATE SENATE 36	x	x									
SD	STATE SENATE 37				x		x					
SD	STATE SENATE 38			x		x						
SD	STATE SENATE 39								x		x	
SD	STATE SENATE 40							x		x		x
SD	ASSEMBLY 66	x							x			
SD	ASSEMBLY 74				x					x		
SD	ASSEMBLY 75		x	x							x	
SD	ASSEMBLY 76						x	x				
SD	ASSEMBLY 77					x						x
U	COUNTY, Unincorporated		x					x				
C	CHULA VISTA			x								
C	LEMON GROVE	x										
R	PORTER VISTA					x						
S	Measure	x	x	x	x	x	x	x	x	x	x	x

C city, M Military, R unincorporated remainder of county, U Unincorporated place in a county.

The test election was modified from the San Diego by combining various districts and races into a selection of ten precincts which concisely included samples of state, statewide district (State Senate and Assembly Districts), judicial, Only five precincts were used in this test (the others are shaded out in the chart above).

Testing was completed using a pre-marked Logic and Accuracy deck. The test deck was used to verify basic election definition and verify the rotation was set up correctly on the all units.

Additional ballots were marked to test response to common voter errors and some ballot tampering changes.

Test Primary ballots cast:

Total cast : 2322
M650 cast: 774
M550 cast: 774

M100 cast: 774

Test General ballots cast (General election ballots used to test different problem conditions caused by voter misstakes or mischief plus environmental problems such as power cutagee.]

Total cast 39
M650 cast: 12
M550 cast: 15
M100 cast: 12

The test deck exercised the following ballot logic and conditions:
Primary party ballots with DTS voting and reporting
Non-Partisan races
Split precinct
Vote for 2 of 5,
Write-in votes (including potential over-vote conditions)
Blank ballots
Rotation based on assembly district at state, state districts, and local levels
Printed ballots were provided in English
Long names in candidate fields. (The preprinted ballot had prototype entries).
Turn-out statistics on final summary reports
Measures
Polls open, close, and report printing.
Review of audit logs.
Consolidating absentee and Election Day precinct voting.

The basic test was repeated using a 300 General Election deck for the same test objectives, less primary unique logic, plus
Power interruptions:

a. M100. Internal battery backup power allowed operations to continue without observed problem.
b. M550. Power loss results in loss of results and election program unless a backup copy of the definition is secured and the latest checkpoint/recovery point is saved to diskette.
c. M650. Same as M550 except that an internal solid state hard drive is available. Saving the results in a Zip disk (recommended) will first save the to the hard drive.