Appendix 2A

Evaluation of Previous Testing – Part 2

THE POLICY INSTITUTE, TRINITY COLLEGE DUBLIN

Mr. Neil McDonnell, *Department of Computer Science, TCD*
Professor Pádraig Cunningham, *Department of Computer Science, TCD*

Table of Contents

Executive Summary

This report presents the findings of a desk-review performed by The Policy Institute (TCD) on behalf of the Commission on Electronic Voting. The desk-review was requested on 21 April 2004, i.e. after the Institute's final research report had been submitted to the Commission, and therefore does not constitute part of the main body of research carried out by the Institute at the request of the Commission.

Documents from three organisations were reviewed. They include reports from Nathean on its desk-review of IES v132, and from ERS on its testing of the count algorithm for IES v124-v129. The broad conclusion from both organisations is that the quality of the IES continues to improve as issues are raised and resolved.

The detailed findings of each report, as they relate to the elections in June 2004, are described in Table 1.

Table 1. Summary of desk-review findings

Nathean Technologies Three reports outlining the results of Nathean's desk-review of IES v132, carried out in April 2004.	***Findings:*** Nathean did not uncover any new issues in its review of IES v132. Progress has been made on resolving 17 previous issues relating to 'best practice' in the design of the IES; 12 of these have now been addressed to Nathean's satisfaction, two have been partially addressed, and three have been closed until after the elections in June 2004. ***Comment:*** The five issues not fully addressed to Nathean's satisfaction are issues of style rather than functionality, and are unlikely to affect the operation of the IES in the elections.
Electoral Reform Services Limited (ERS) One report outlining the results of testing on the count algorithm in IES v124-v129, carried out in March 2004.	***Findings:*** In its testing of the count algorithm, ERS added thousands of new and altered test cases. These uncovered a number of minor faults in the count software. Following a number of new releases from the developer, all test cases passed successfully against IES v129. ***Comment:*** One problem found by ERS has persisted, and has occurred again in testing by The Policy Institute on IES v131. This is a 'rounding error' that can cause surplus remainder votes to be transferred to the wrong candidate. Several attempts to fix the problem have already been made, some of which introduced new faults into the software. This highlights the desirability of full testing on the *final* version of the IES approved for use in the June 2004 elections.

PMI Software Six reports from 2001 describing the results of an early review of the IES.	***Findings:*** • The suitability of MS Access 97 as the back-end database for the IES was confirmed. Access 97 databases were also found to have sufficient capacity to handle the volume of data required by the IES. • It was confirmed that before votes are counted, they are mixed by the IES in a statistically random manner. ***Comment:*** The structure of IES databases may have changed since 2001. Confirmation that no capacity problems can occur with the databases used in v132 might help increase confidence in the system.

1 Introduction

1.1 Objective of report

Over the period of March/April 2004, The Policy Institute, TCD carried out a body of research on behalf of the Commission on Electronic Voting. Following submission of the Institute's final report, the Commission requested that it undertake additional work, namely, a desk-review of a number of documents relating to electronic voting that were received by the Commission in early April.

This review would:

- Summarise the purpose and scope of each of the 10 documents supplied;
- Summarise the findings of each report; and
- Comment on the relevance of these findings for the elections in June 2004.

This report describes the outcome of this desk-review. It is based on desk research and was prepared over the period 21-27 April 2004.

1.2 Documents desk-reviewed

The following documents were reviewed for this report:

Table 2. Summary of documents desk-reviewed for this report

Company	Report(s) reviewed	Report Date
Nathean	1. Code Review of IES Build 0132 – Irish Election Processing. 2. Code Review of IES Build 0132 – Election Setup & Maintenance. 3. Code Review of IES Build 0132 – Vote Reader. *These three reports describe the results of Nathean's desk-review of IES v132.*	20-04-2004 20-04-2004 20-04-2004

Company	Report(s) reviewed	Report Date
ERS	Report on Irish STV Software Testing. *Describes the results of testing carried out on the count software for IES versions v124-v129.*	March 2004
PMI	1. Code Review of the Powervote Electronic Voting System. 2. Evaluation of Integrated Election Software Database. 3. Evaluation of Integrated Election Software Development Environment. 4. Code Review Guidelines for Powervote Electronic Voting System. 5. PMI Software's Pseudo-code for Code Reviewing. 6. Evaluation of Random Number Generation in the Powervote Electronic Voting System. *These describe the results of an early review of the IES. Some findings of the review are now out-of-date, while others remain valid.*	14-12-2001 14-12-2001 14-12-2001 14-12-2001 14-12-2001 14-12-2001

1.3 Approach and method

The reports from each organisation are reviewed in turn. The structure of the reviews for Nathean, ERS and PMI is as follows:

1. Description of report. The purpose and content of each report is described.
2. Findings of report. Each report's findings and conclusions are summarised.
3. Comment on findings. The findings of each report are evaluated with respect to their relevance for the Nedap/Powervote electronic voting system proposed for use in Ireland's elections in June 2004.

1.4 Structure of report

There are three further sections in this report:

- Section 2 examines Nathean's three desk-review reports.
- Section 3 examines the ERS testing report.
- Section 4 examines PMI's six reports from 2001.

Each section draws its own conclusions, and a summary of the main issues is contained in the Executive Summary.

2 Review of reports from Nathean Technologies

2.1 Description of reports

Nathean Technologies had previously carried out a number of desk-reviews of the IES software. The reports reviewed here (dating from April 2004) set out the results of its desk-review of the

latest release of the IES (v132). The results are presented in three reports, each dealing with one aspect of the IES:

1. Code Review of IES Build 0132 – Irish Election Processing [ref. 4[1]].
2. Code Review of IES Build 0132 – Election Setup & Maintenance [ref. 5].
3. Code Review of IES Build 0132 – Vote Reader [ref. 6].

2.2 Findings of reports

1. Code Review of IES Build 0132 – Irish Election Processing.
   No new issues were found during this review. Four issues relating to 'best practice' were outstanding from previous reviews, but all have now been addressed to Nathean's satisfaction.

2. Code Review of IES Build 0132 – Election Setup & Maintenance.
   No new issues were found during this review. A number of issues were outstanding from previous reviews and fall into two categories:

   - *Issues relating to best practice*. Some 17 issues were raised in previous reviews, of which 12 have now been addressed to Nathean's satisfaction. Another two (relating to exception handling) have been addressed by the developer, but not entirely to Nathean's satisfaction. The remaining three (relating to stylistic issues in the IES design) have not yet been addressed, and have been closed until after the June 2004 elections.
   - *Issues relating to functionality*. Eight issues were raised in previous reviews; all have now been addressed to Nathean's satisfaction.

3. Code Review of IES Build 0132 – Vote Reader
   No new issues arose during this review, and issues raised during previous reviews have been addressed to Nathean's satisfaction.

2.3 Comment on findings

In its review of the 'Election Setup and Maintenance' parts of the IES, Nathean highlighted five issues that have not been fully resolved to its satisfaction. As described above, these relate to 'best practice' in software design.

The concept of 'best practice' is not precisely defined, and diverse views on the appropriateness or otherwise of particular code structures can be held by different software practitioners. Regardless of the detailed arguments in this case, it does not appear that the issues raised by Nathean would impact on the normal operation of the IES during the June 2004 elections. This is because they relate to the style of the software rather than its functionality.

3 Review of report from Electoral Reform Services Limited (ERS)

3.1 Description of report

The report describes the testing performed by ERS on the election count software in the IES

[1] Referenced documents are listed in Appendix A in alphabetical order.

(versions v124-v129). The approach taken by ERS is to perform 'comparison testing': several thousand test cases (sample elections) are counted by the IES and by ERS's own implementation of the Irish PR-STV algorithm. The results are compared, and any discrepancies noted. If a discrepancy cannot be accounted for by ERS, this indicates the presence of a fault in the IES.

3.2 Findings of report

In its previous test report [ref. 3, p.7], ERS stated: "We suspect that if it were practical to run several thousand, rather than several hundred, test cases through IES, then we might find an error". ERS has added several thousand new or altered test cases in its latest testing, and several new faults were found.

Errors found during testing are divided into four categories:

1. **Presentational errors**: These are errors in the intermediate screens that display the detailed progress of a count, and do not affect the result. ERS did not specifically search for presentational errors, but reported them to the developer when they were noticed. All reported presentational errors were fixed in IES v129.
2. **Operational errors**: These errors "hinder the operation of the software rather than cause errors in the result sheet" [ref. 2, p.5]. Several such errors were encountered during testing, and one remains in the software: the Microsoft Access 97 database used to store voters' preferences during a count has a maximum size of 1GB. This could be exceeded if an election with several hundred thousand votes underwent repeated re-counts. This problem "should not occur in a real election since the election would be counted only once. If it did occur then the solution would be to use the Microsoft Access "compact and repair" function to reduce the database back to the size it was when the votes were first imported" [ref. 2, p.5].
3. **Rounding errors**: These errors "caused the count software to make the wrong choice when allocating surplus remainder votes" [ref. 2, p.5], and might have influenced the outcome of an election count. They occurred because "some arithmetic functions had been poorly implemented in earlier versions" of the IES. Rounding errors occurred in testing of v124, v125, v126 and v128. The original fault was identified in v124; subsequent errors were due to faulty attempts to fix the problem.
4. **Count logic errors**: These are logical errors that occur when the IES fails to properly follow the Irish PR-STV rules. One such error occurred in testing of v125. It could not have affected the result of an election, however, since it "concerned the distribution of surpluses after all candidates are deemed elected" [ref. 2, p.5].

The developer addressed all faults identified by ERS, and all test cases passed successfully using IES v129. ERS concluded that there are now "exceptionally strong grounds for believing that IES v129 is a sound implementation of Irish STV count rules", and that "the risk of IES v129 producing an incorrect result sheet in an actual Irish election is now probably less than 1 in 10,000 cases" [ref. 2, p.5].

3.3 Comment on findings

- **Operational error caused by limitation in MS Access 97 database size.**
  In 2001, PMI Software looked at the question of whether an MS Access 97 database might exceed its maximum size during operation. Its conclusion was that Access would handle the

volume of data "required by the IES application in a stable manner without exceeding any of its size constraints" [ref. 9, p.9]. This issue is discussed further in Sections 4.2 and 4.3, Point 2.

- **Rounding fault in calculation of transfer factors during a count.**
  This fault can cause surplus remainder votes to be transferred to the wrong candidate, and could therefore be more serious. It arose originally in a very small number of cases – 2 out of 5,274 tests run on IES v124. Faults of this nature are commonly found during testing. After the fault was raised in v124, however, the fix inserted by the developer for v125 actually introduced a new fault. The fix inserted for v126 also introduced new faults, and caused several test cases to fail that had previously passed. The fix inserted for v128 was also not correct. Only with v129 did ERS believe the problem had been resolved. Best practice in the software industry suggests that great care should be taken to verify that fixes are complete and correct before they are released. Even after v129, however, the rounding problem seems to have persisted and has arisen again in testing by the Policy Institute on IES v131 [ref. 14].

  New versions of the IES continue to be released, with each new version containing fixes for problems found in the previous one. Each fix can also introduce new faults, and the evidence suggests that this has, in fact, been occurring. When final testing has been completed for the version of the IES approved for the elections in June 2004, any new fixes (releases) should trigger complete re-testing of the IES.

4 Review of reports from PMI Software

4.1 Description of reports

PMI Software performed a series of desk-reviews on the IES in 2001. It also evaluated the database solution employed, and looked at the software development environment used by the developer to design the IES.

A total of six reports were presented:

1. Code Review of the Powervote Electronic Voting System [ref. 8].
   Three areas of the source code were inspected:
   - Business logic of the count process;
   - Data module of the count process; and
   - Business logic for data transfer between ballot modules and the IES database.

   The IES has undergone substantial change since 2001, and so many of the issues raised by this report are no longer relevant.

2. Evaluation of Integrated Election Software Database [ref. 9].
   The appropriateness of MS Access 97 as the back-end database for the IES is evaluated. This report remains valid today.

3. Evaluation of Integrated Election Software Development Environment [ref. 10].
   The design environment used by the developer to produce the IES is evaluated. This report remains valid today.

4. Code Review Guidelines for Powervote Electronic Voting System [ref. 11].

This report outlines the process followed by PMI during the code review. It is no longer relevant.

5. PMI Software's Pseudo-code for Code Reviewing [ref. 12].
   As part of its review of the IES, PMI produced a pseudocode version of the PR-STV algorithm. This report simply presents a copy of the pseudocode as a reference for future reviewers. It does not make any findings.

6. Evaluation of Random Number Generation in the Powervote Electronic Voting System [ref. 13].
   This report evaluates the 'mixing and numbering' function in the IES that randomises votes prior to the election count. Its findings remain valid today.

4.2 Findings of reports

Only those findings that remain relevant today are presented here.

1. Code Review of the Powervote Electronic Voting System.
   - The report raises the absence of consistent exception handling (i.e. error handling) in the code as an important issue.
   - The source code responsible for transferring data between the ballot module and the IES database is reported to be written in Dutch. This "obviously makes it very difficult to work out all the functionality contained in the unit" [ref. 8, p.85].

2. Evaluation of Integrated Election Software Database.
   - Overall, the report finds that MS Access 97 is suitable for use with the IES. As mentioned in Section 3.3 above, it also concludes, "Access will handle the volume of data that will be required by the IES application in a stable manner without exceeding any of its size constraints" [ref. 9, p.9]. The capacity of the IES database is reported as being sufficient to hold the preferences for 7½ million voters [ref. 9, p.5].
   - Doubts are raised about the security of MS Access 97. Databases are password protected but are not encrypted. Passwords can be easily identified using free software from the Internet – this finding was also verified by internal research carried out by The Policy Institute during March/April 2004 at the request of the Commission on Electronic Voting.
   - Doubts are raised about two aspects of the IES database structure: lack of primary keys in IES tables, and lack of referential integrity to enforce consistency between tables. These relate to 'best practice', and are highlighted as "possible design flaws" [ref. 9, p.9].

3. Evaluation of Integrated Election Software Development Environment.
   - Borland Delphi 5, Opus DirectAccess, and TurboPower's Async Professional are the development tools used to produce the IES. PMI concludes that all three are excellent.

4. Code Review Guidelines for Powervote Electronic Voting System.
   No longer relevant.

5. PMI Software's Pseudo-code for Code Reviewing.
   No findings in this report.

6. Evaluation of Random Number Generation in the Powervote Electronic Voting System.
   - Delphi's random number generator is seeded with the value of the system clock, and produces pseudo-random numbers using the Lehmer algorithm. The sequence of numbers generated is statistically random as required by the mixing function. This is important because non-random mixing of votes prior to counting could affect the outcome of an election.
   - After all votes have been mixed, there is no way to work backwards from the database to recover the original order of the votes.

4.3 Comment on findings

1. Code Review of the Powervote Electronic Voting System.
   - The absence of consistent exception handling in the IES has remained an issue with reviewers up until today; it was raised most recently by Nathean in its code review of v132 (see Section 2.2, Point 2).
   - PMI reports that its desk-review of the IES function responsible for reading votes from ballot modules was hampered by the fact that it is written in Dutch. Nathean has carried out more recent code reviews of the IES, and has stated in private correspondence that it procured the services of a Dutch-speaking code reviewer to address the problem.

2. Evaluation of Integrated Election Software Database.
   - The report states that the IES database (Results_Ballots) has sufficient capacity to store votes for up to 7½ million voters. If the database structure has changed since 2001, however, its capacity may also have changed. Nathean has not highlighted any potential problem in this area in its architectural assessment of the IES [ref. 7]. Nevertheless, it might help to increase confidence in the system if it were confirmed that the current database structure would not give rise to capacity problems, even in elections involving hundreds of thousands of voters.
   - The potential security vulnerabilities of MS Access 97 have been addressed by the DoEHLG through tight physical security: "PCs used for the election set-up and vote counting are stand-alone machines complete with anti-virus software and each one will be "security hardened" for the election. This means that all unnecessary services and programs on the PC will be disabled or reconfigured to prevent any access to the PC. A two factor security procedure will be required to login to the PCs" [ref. 1, p.7]. The security of the databases (and all IES software) is therefore to be assured by the fact that they will be inaccessible to unauthorised personnel.
     Nathean has also raised the issue of database security [ref. 7, p.11]. A response from the developer has been deferred until after the election in June 2004 [ref. 5, p.8; ref. 7, p.4]. Nathean accepts that database security is "adequate in its current form (assuming strong physical and networking security measures are in place)" [ref. 7, p.3].
   - The fact that the IES does not use primary keys or referential integrity in its databases has also been raised by Nathean [ref. 7, p.11]. This is a question of 'best practice', and is therefore open to some dispute. PMI admits as much, stating that "the presence of Primary Keys is not required", and "it is not necessarily wrong to have no referential integrity" [ref. 9, p.8]. A response by the developer to this issue has also been deferred until after the election in June 2004 [ref. 7, p.11]. The issue should not have any bearing on the operation of the IES.

3. Evaluation of Integrated Election Software Development Environment.
   -

4. Code Review Guidelines for Powervote Electronic Voting System.
   -

5. PMI Software's Pseudo-code for Code Reviewing.
   -

6. Evaluation of Random Number Generation in the Powervote Electronic Voting System.
   - The fact that the original order of votes cannot be recovered from the preferences database after it has been mixed means that the database can be published without it being possible to re-sort votes into the order in which they were read from ballot modules. Since the order of votes on ballot modules is also random [ref. 15, p.40], voter anonymity is therefore protected by two separate randomisation steps.

Appendix A Referenced documents

No.	***Company***	***Title***	***Date***
1	DoEHLG	*Security and Audit Features of the Election Management System*	January 2004
2	ERS	*Report on Irish STV Software Testing*	22-03-2004
3		*Report on Irish STV Software Testing*	15-12-2003
4	Nathean	*Code Review of IES Build 0132 – Irish Election Processing*	20-04-2004
5		*Code Review of IES Build 0132 – Election Setup & Maintenance*	20-04-2004
6		*Code Review of IES Build 0132 – Vote Reader*	20-04-2004
7		*Architectural Assessment & Code Review of IES for use at June 2004 Elections (Build 0111)*	23-12-2003
8	PMI	*Code Review of the Powervote Electronic Voting System*	14-12-2001
9		*Evaluation of Integrated Election Software Database*	14-12-2001
10		*Evaluation of Integrated Election Software Development Environment*	14-12-2001
11		*Code Review Guidelines for Powervote Electronic Voting System*	14-12-2001

No.	***Company***	***Title***	***Date***
12		*PMI Software's Pseudo-code for Code Reviewing*	14-12-2001
13		*Evaluation of Random Number Generation in the Powervote Electronic Voting System*	14-12-2001
14	Policy Institute, TCD	*Work Strand 1.1: Validity of the electronic implementation of STV election counts in Ireland*	15-04-2004
15	PTB	*Test Report 2 – Voting machine ESI2 – Software for elections in Ireland*	17-09-2003