

Appendix 2C

Evaluation of Voting Machine, Peripherals and Software

THE UCD/MIT/ESRI RESEARCH GROUP

Richard Sinnott
Ted Selker
Bil Lewis
Brendan Whelan
James Williams
James McBride

Table of Contents

Executive Summary	155
1 Introduction.....	157
2 Summary of Previous Test Reports.....	158
2.1 “Tests on the Design of a Voting Machine” Physikalisch-Technische Bundesanstalt, 1998, 2003.....	158
2.2 Critical Requirements	159
2.3 Recommendations.....	159
2.4 “Code Review of IES Build 0111” Nathean Technologies, 2003	159
2.5 “Report on Irish STV Software Testing” Wadsworth, Wichmann. ERS, 2003	159
2.6 “Electronic Voting Security Assessment” Zerflow Ltd., 2003.....	159
2.7 PTB-Test Report 2, 17 September 2003	160
3 Process Overview.....	160
4 Vulnerabilities.....	162
5 Input-Output test of voting machines	167
5.1 Objective	167
5.2 Experimental Design.....	167
5.3 Sampling	168
5.4 Preparation of the Test Materials and Interviewer Training.....	169
5.5 The Parallel Videotaped Experiment	170
5.6 Results.....	171
5.7 Conclusion	178
6 Using IES from the Local Electoral Area/ Constituency Worker’s Perspective	179
6.1 Critical requirement	182
6.2 Recommendations.....	182
7 Using IES from the Service Centre Worker’s Perspective.....	182
7.1 Critical Requirements	183
7.2 Recommendations.....	183
8 Using the Voting Machine from the Poll Worker’s Perspective.....	184
8.1 Setting up the machine.....	184
8.2 Opening the Poll	185
8.3 Running the poll.....	185
8.4 Closing the poll.....	185
8.5 Critical Requirements	185
8.6 Recommendations.....	185
9 Using the Voting Machine from the Voter’s Perspective.....	186
9.1 Recommendations.....	187
10 Documentation	188
11 Security Measures.....	189
11.1 Critical Requirements	190
11.2 Recommendations.....	190
12 Conclusion	190
The Research Team.....	191

Executive Summary

- In response to an invitation from the Commission on Electronic Voting and following discussions with the Commission, the Institute for the Study of Social Change at University College Dublin assembled an inter-disciplinary and inter-institutional team to conduct research on behalf of the Commission. The objective of the research was to contribute to the Commission's evaluation of the accuracy and secrecy of the system of electronic voting proposed for use in the European and local elections of June 2004. It is important to emphasise that this is a *contribution* to the Commission's evaluation and is not, in itself, an end-to-end test of the system. In particular, we have not undertaken any detailed testing of the software for counting the votes. Our understanding is that this and other aspects of the proposed system are being tested by other groups or agencies retained by the Commission. Our conclusions must be read in the light of this division of labour.
- The research team was drawn from three institutions: University College Dublin (UCD), the Massachusetts Institute of Technology (MIT), and the Economic and Social Research Institute (ESRI).
- This report concentrates mainly on black box testing. In terms of code review, it draws on previous reports commissioned by the Department of Environment, Heritage and Local Government (DOELG). We have also conducted a limited review of the vote-counting source code; for reasons of confidentiality, the report of the outcome of that code review has been sent directly to the Commission on Electronic Voting.
- We have reviewed six reports on the Nedap/Powervote electronic voting system. These previous studies demonstrate that the voting hardware is electrically compliant with standards. They show that the software works and is reasonably structured.
- A brief consideration of the process of preparing and running an election and counting the votes enables one to identify the potential vulnerabilities of the system. There are two main types of attacks that can be launched against a voting system. The attacker can (a) produce a Fraudulent Count (get the wrong person declared the winner) and (b) prevent voters from voting (commonly known as a "Denial of Service" attack).
- Within these broad categories, there are so many different conceivable attacks that, at first glance, it might seem impossible to adequately protect against all of them. However, testing the machines before the election can find all but the attacks that add batteries and clocks to the voting machine. Parallel testing would detect even these problems.
- As part of the testing process, we conducted an input-output comparison of a representative sample (N=739) of the almost 7,000 machines that have already been deployed around the country in preparation for the June 2004 elections. In all, 36,950 simulated ballots (50 per sampled machine) were entered and verified by teams of interviewers drawn from the ESRI's national panel of interviewers in collaboration with Returning Officers or their representatives in each centre. In addition to the main field experiment, a smaller parallel exercise was undertaken in the ESRI's offices in Dublin. This more limited experiment (involving the input of 5,000 votes on 5 voting machines) was videotaped throughout.

- The results of the input-output test showed that 36,831 or 99.68% of the 36,950 target votes prepared for inputting into the machines duly turned up as votes correctly recorded on the ballot modules. This level of accuracy in the input and recording of votes is sufficient to rule out any substantial fraud or machine error affecting the deployed machines.
- However, an appreciable level of error (0.32%) did occur and the errors took a number of forms – votes omitted which should have been entered, extra votes appearing which were not in the target set and erroneous entries. On detailed examination (see full report below), all of these errors appear much more likely to have arisen from predictable mistakes by the operators as they entered the preferences than from any other sources. Video evidence supports this view by showing that, even in the very carefully controlled video-taped experiment, all six discrepancies (out of 5000) were attributable to human error.
- Our analysis of the input errors arising suggests certain issues that deserve attention in programmes designed to educate voters or train election staff. It also suggests issues that should be tackled in any further evaluation of the usability of the machine.
- The occurrence of errors in our experimental input process indicates that very careful attention will need to be paid to the inputting of postal votes in the electronic system.
- On balance, however, the results of the input-output test indicate that the voting machines deployed for use in the June 2004 European and Local elections are a reliable means of recording the votes of the people.
- In addition to the input-output test of the voting machines, this project conducted a series of tests of the usability of the system. The findings of these tests can be summarised by citing the main critical requirements arising from them.
 - All personnel who use the IES system must demonstrate proficiency in hands-on, timed tests.
 - The results file must be backed up on two disks when created, one stored off site. It is further critical that the disk is authenticated when it is about to be used.
 - The label for the ballot modules should extend over the “top” of the ballot module, so that it acts as a seal and so that the identification of the designated polling station is obvious at all times.
 - The IES 126 software should never be used for setting up or processing the results of an election without two people at the workstation agreeing about each step.
 - The control unit (which controls the selection of the races available to each voter and determines the disposition of incomplete ballots [those that have not been confirmed by a second push on the cast vote button]) requires continuous oversight by at least one other person.
 - In order to prevent erasure of the backup modules, when the poll is closed, the electricity supply to the voting machine must be discontinued and the module must be sealed.
 - All backup modules must have serial numbers.
- We conclude (a) that the voting machines deployed for use in the June 2004 European and Local elections are a reliable means of recording the votes of the people and (b) that, provided that our critical requirements are implemented and that the aspects of the system we have not examined are shown to be satisfactory, the chosen electronic voting system can be safely used in the June 2004 elections.

1 Introduction

In response to an invitation from the Commission on Electronic Voting and following discussions with the Commission, the Institute for the Study of Social Change at University College Dublin assembled an inter-disciplinary and inter-institutional team to conduct research on behalf of the Commission. The research team was drawn from three institutions: University College Dublin (UCD), the Massachusetts Institute of Technology (MIT), and the Economic and Social Research Institute (ESRI).

The objective of the research was to contribute to the evaluation of the accuracy and secrecy of the system of electronic voting proposed for use in the European and local elections of June, 2004, i.e. the Nedap ESI2 Voting Machine and the Powervote Integrated Election Software (IES) v126. It is important to emphasise that this is a *contribution* to the Commission's evaluation and is not, in itself, an end-to-end test of the system. In particular, we have not undertaken any detailed testing of the software for counting the votes. Our understanding is that this and other aspects of the proposed system are being tested by other groups or agencies retained by the Commission. Because this investigation specifically looks for potential problems in the system, it has at times a fairly negative tone. Nonetheless, we believe that, if the critical issues identified below plus those identified by other agencies retained by the Commission are satisfactorily dealt with, the system is capable of giving Ireland its most accurate and efficient election to date. In this context, it is worth noting that the Irish electoral system (proportional representation by means of the single transferable vote (PR-STV)) is a complex and sophisticated voting system¹ that would benefit considerably in terms of accuracy and efficiency from the introduction of electronic voting².

If everything in an election were to run perfectly – an average number of candidates, straightforward nomination processes producing full candidate details with good photographs, a well-trained and healthy staff at all levels, a knowledgeable and involved electorate, no clever attackers, we wouldn't need a report such as this. Our objective, however, is to consider the system as it could behave under the worst of circumstances – with the poorest trained staff and the cleverest attackers.

We begin with a brief summary of previous studies of the system commissioned by the Department of the Environment, Heritage and Local Government (DOEHLG) and review the sequence of events involved in preparing and running an election. We then consider the potential vulnerabilities of the system (vulnerabilities both to malicious parties and to unintentional misuse). This leads us first to conduct an input-output test of a representative sample of voting machines in order to determine whether the output corresponds to the input or whether, through malfunction or through interference, there are systematic distortions in the recording of the votes of the people. We then analyse the system from the point of view of the various users of the system (those responsible for preparing the election, those who supervise and run the system on voting day, the voters themselves and those who conduct the count). The simpler a system is, the harder it is to defraud, and the less likely it is that legitimate users will make mistakes. At times we will delve into low-level detail (Does the voter have to press "Cast Vote" button once or twice? Are the LED displays clear

¹ For an overview of the system, see Richard Sinnott, "The electoral system" in John Coakley and Michael Gallagher, eds., *Politics in the Republic of Ireland*, 3rd edition, London: Routledge, 1999, pp. 99-127.

² These gains have to be weighed against a likely loss in the public's sense of involvement in and understanding of the process of counting votes and a consequent loss in their overall understanding of the electoral system. If electronic voting goes ahead, measures would need to be taken to minimise that loss.

enough?). Details such as these have been responsible for loss of votes by confused voters in electronic elections elsewhere.

Along the way we make many recommendations. Those that are critical to knowing and demonstrating that voter intentions have been recorded and counted accurately we refer to as “Critical Requirements.” Suggestions for improvement are simply labelled “Recommendations.”

Evaluation of a system such as that under consideration should involve a combination of “black box” testing and code review. The black box testing (where the tester gives the system a wide range of input data to see if it handles it correctly) allows us to state that the system is behaving as it was designed to behave. Code review (where the tester looks at the construction of the system, particularly the software) allows us to state that the program is written in a manner that can be maintained and allows bugs to be easily found. This report concentrates mainly on black box testing. In terms of code review, we draw on previous reports commissioned by the Department of the Environment, Heritage and Local Government (DOELG). We have also conducted a review of the vote counting source code; for reasons of confidentiality, the report of the outcome of that code review has been sent directly to the Commission on Electronic Voting.

This report is the result of the intense efforts of a small team working under tight time restrictions. We are confident that all of our high-level points are relevant, accurate, and important. Still, there is some likelihood that we have missed some details of the system or made recommendations that have been adequately addressed already. We also note our regret that, due to the time constraints, it has not been possible to test the equipment with actual voters, ballot workers, and election officials. Some of the findings of our black-box efforts underline the desirability of such hands-on testing.

2 Summary of Previous Test Reports

We have reviewed five reports on the Nedap/Powervote electronic voting system. The issues they raise point to things to beware of, but none of them lead to predictions of dire consequences. These previous studies demonstrate that the voting hardware is electrically compliant with standards. They show that the software works and is reasonably structured.

2.1 “Tests on the Design of a Voting Machine” Physikalisch-Technische Bundesanstalt, 1998, 2003

The Physikalisch-Technische report covered black-box testing of the voting machine and provided an extensive physical report (electrical, physical, environmental). This report found no problems that would make the voting machines unusable. However, it pointed to several issues regarded as serious:

- Error code numbers are displayed and must be looked up in a list. This complicates the process of understanding and solving the problem.
- “In cases of successful restoration [of a vote], there are no messages.” (If the user is not 100% certain that the restoration has been successful, then it isn’t successful.)

- The voting machine ID can be changed. This could allow undocumented exchange of machines. Even if not fraudulent, exchanging machines needs to be documented to be done without error or risk.
- There are two serial ports on the voting machine. How they might be used is an important issue.
- The voting machine backup module is cleared when a new ballot module is inserted. This seems to create the possibility of inadvertently destroying backup data.
- “In certain cases the voting machine may be used to a reduced extent.” (Any variation in the behaviour of the machine is a source of potential complications and errors.)

2.2 Critical Requirements

- The identification number of a voting machine should not be modifiable after certification.
- Exposed serial ports must be shown to be incapable of altering the voting machine.

2.3 Recommendations

- Explicit resets of the backup data by a poll worker should not be possible.

2.4 “Code Review of IES Build 0111” Nathean Technologies, 2003

Nathean Technologies did not find any particularly serious problems in the voting administration software. They do make reference to a “LOCAL_LEVEL compiler directive.” This implies that the compilation of the local level software is somehow different from the rest of the software. While this is not necessarily a problem, a reason and documentation should be provided when things are compiled separately.

2.5 “Report on Irish STV Software Testing” Wadsworth, Wichmann. Electoral Reform Society, 2003

The ERS report describes a wide range of tests of the counting software for IES versions 93 and 121. Their conclusion is that the voting software functions correctly. They found v121 to behave as required over a wide range of sample elections. The only reservation we have is the statement in appendix D: “Such a situation seems hardly credible in a public election and so most of these cases were excluded.” We believe that the software should behave correctly even in “hardly credible” cases (such as the California recall election which had 134 candidates).

2.6 “Electronic Voting Security Assessment” Zerflow Ltd., 2003

A 2002 assessment of the system by Zerflow made a number of suggestions, all of which were addressed to their satisfaction by 2003. We feel that several of their concerns need more attention. In particular:

- The process of doing an audit is not laid out in the documentation (however, we understand that the audit issue is being dealt with by other research teams on behalf of the Commission).
- In the case of a voting machine failure during an election, it is not clear how that machine should be handled, where it should be stored, when its ballot module should be removed, etc. (attackers must be kept from getting to vote on the machine in a back room).
- Zerflow states, “Only the returning officer or person authorised by him/her is permitted to wipe the backup cartridge.” The process must insure that unauthorised people do not have the opportunity to do this.

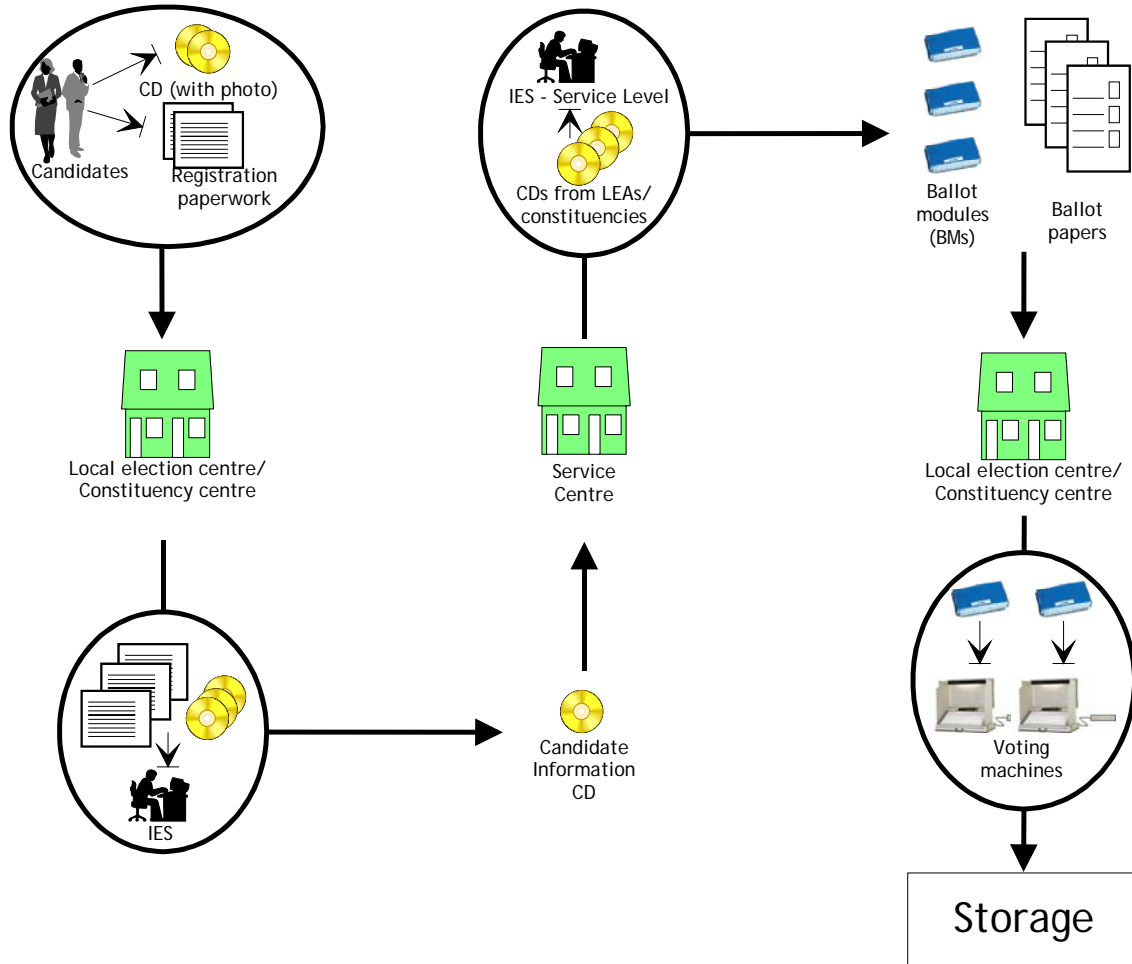
2.7 PTB-Test Report 2, 17 September 2003

This report looked at the details of the voting machine software, reviewing the C code for the entire voting machine. They conclude that the system is well built, conforming to standard programming practices and fully compliant with the requirements.

3 Process Overview

1. The first step in the election process (as illustrated in Fig. 1) is for the candidates to register their intention to run by doing whatever paperwork is required (not governed by IES) and bringing an appropriate photograph of themselves to either the Local Electoral Area (LEA) centre or the constituency centre.
2. The candidate’s information (name, party, address, etc.) is entered into the IES by a person at the centre. The candidate’s picture is copied from the Compact Disk (CD) that the candidate brings together with other necessary information.
3. When all candidate information has been entered and the “end of registration” period arrives, the information is written to a CD.
4. The CD is transferred to the Service Centre.
5. The service centre collects CDs and ballot papers from all constituent Local Electoral Areas/constituencies.
6. All the information is entered into the IES at “Service Level” and the “Ballot Modules” are created, one for each voting machine. All of the Ballot Modules for a polling station contain identical information. All polling stations in a local electoral area will also have identical information on their Ballot Modules. The data for the Ballot Modules are checked against the Ballot Papers.

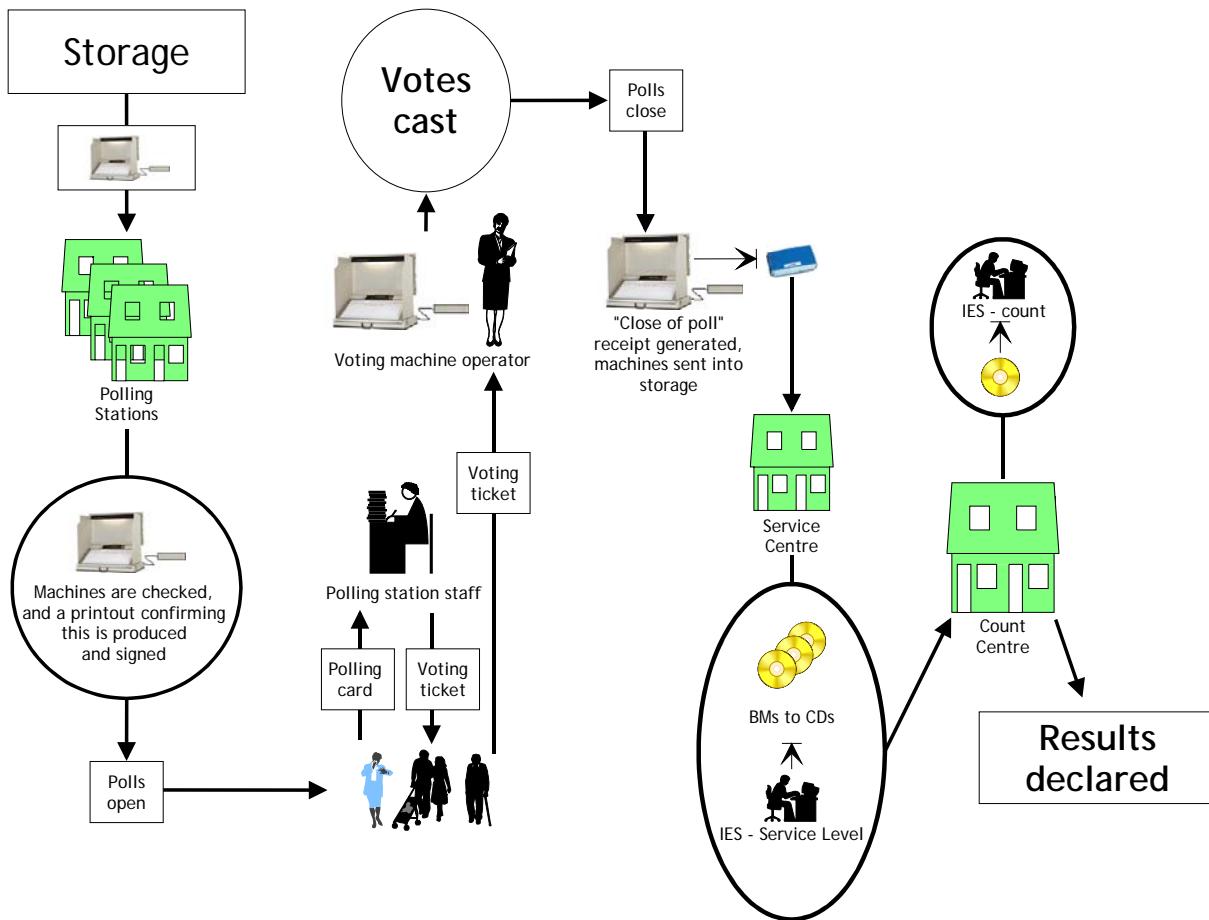
Figure 1: Preparing for the Election



7. The Ballot Modules are sent back to the local levels.
8. At the local levels, the Ballot Modules are placed in the Voting Machines, as are the Ballot Papers. The Ballot Modules (in the Voting Machines) are checked against the Ballot Papers.
9. The Voting Machines are then sealed and transferred to secure storage, with the Ballot Modules inside.
10. When election time arrives, the Voting Machines are moved to the various polling stations (Fig. 2). They are set up, checked, and a printout showing identification numbers, candidate details, and showing that there are no votes already recorded on the ballot module is produced and signed. The machines are then put into operation.
11. Voters come in and have their registration verified by existing means. They receive a voting ticket from the official and proceed to the designated Voting Machine. The operator of the Voting Machine selects the appropriate set of races for them to vote on; they then enter their preferences and cast their vote(s).

12. At the end of the polling day, the polls are closed, a “close of poll” receipt is generated, the Voting Machines are shut down and the Ballot Modules are removed.
13. The Voting Machines are transferred back to secure storage (with the backup modules still inside), while the Ballot Modules are returned to the Service Centre.
14. At the service centre, after the contents of all the Ballot Modules are read in, the operator writes out a series of CDs containing the votes from the appropriate Ballot Modules, one CD for each Local Electoral Area or constituency.
15. The CDs are sent to the appropriate Local Electoral Area/constituency count centre.
16. The operators in the Local Electoral Area and constituency count centres read in the CD and execute the count.
17. The winners are announced from the Local Electoral Area/constituency count centre.

Figure 2: Election and Post-Election Processing



4 Vulnerabilities

Protection of the process is critical; without it the system becomes vulnerable to attackers. We must assume that the attacker has full access to sample machines, spare Ballot Modules, the source code,

all the documentation, lots of money and insider knowledge. (We should point, however, that, to date, we know of no malicious attacks on any electronic voting machines in any country).

There are two main types of attacks that can be launched against a voting system. The attacker can (a) produce a **Fraudulent Count** (get the wrong person declared the winner) and (b) prevent voters from voting (commonly known as a “**Denial of Service**” attack).

The following are the main components of the system that can be attacked:

- The IES software could be attacked (a) inside the manufacturing company (either by an employee or a clever internet hacker), (b) during delivery (switching CDs in the post, etc.), (c) in the PC at the election centre.
- The Programming/Reading Unit (PRU) could be attacked in similar fashion.
- The Voting Machine could be attacked (a) inside the manufacturing company, (b) during delivery, (c) during setup, (d) in storage (either before or after the election), (e) at the polling station, (f) during transportation to or from storage.
- The Ballot Module could be attacked (a) inside the manufacturing company, (b) during delivery, (c) during programming, (d) during setup, (e) in storage (before or after the election), (f) at the polling station, (g) during transportation from storage, (h) during transportation back to the Service Centre, (i) during reading at the Service Centre, (j) after the election.
- The Ballot Paper could be attacked (a) during production at the Election Centre, (b) during printing, (c) during transport, (d) during installation, (e) during voting, (f) after the election.
- The CDs that are sent to the Service Centre with the candidates’ details could be attacked (a) during transportation, (b) after the election.
- The CDs that are sent to the Counting Centres (from the Service Centre) with the details of the votes could be attacked (a) during transportation, (b) after the election.

An effective **Fraudulent Count** must be undetected. Fraudulent Count attacks can be launched against:

- The IES software, by distorting the reading/recording of the Ballot Modules at the Service Centre, or by faking the count at the Count Centres.
- The PRU, by having it distort the reading of the Ballot Modules.
- The Voting Machine, by changing the EPROM programs to misrecord data on the Ballot Modules.
- The Ballot Modules, by replacing the internal components with different ones that will report what the attacker wants.
- The Ballot Papers, by switching candidate positions on the paper, or by removing or

replacing candidates on the paper.

- The CDs with the votes, by replacing them with CDs containing different counts.

Denial of Service attacks can be launched against:

- The IES software, by preventing it from producing the correct Ballot Papers or Ballot Modules.
- The PRU, by preventing it from producing the correct Ballot Modules.
- The Voting Machine, by disabling it somehow (breaking it, cutting cables, causing short-circuits).
- The Ballot Modules, by disabling them (e.g., sticking toothpicks into the connector), or by stealing them.
- The Ballot Papers, by damaging them (covering them up with tape, pouring ink over them).
- Both sets of CDs, by stealing them, damaging them.

Figure 3: Insides of a Ballot Module



A great number of these attacks are not viable; either they are too difficult to carry out, too easy to detect, or do too little damage. Our objective is to ensure that there are reasonable measures in place to make all of these attacks non-viable. As the ability to maintain secrecy drops rapidly with increasing numbers of people, we are primarily concerned with attacks that can be carried out effectively by a small number of people. This eliminates a lot of the attack targets.

Attacking the Ballot Papers would require a large number of people and would be readily detectable. Existing safeguards seem sufficient. Attacking the CDs seems equally unlikely. There are too many safeguards in the system and it's too easy to detect. A possible Fraudulent Count attack on the Ballot Modules could be mounted by replacing their memory chips with a computer chip running a malicious program. That program would be able to record votes anyway the attacker

desired. Because the candidates' parties are recorded on the ballot module, the attacker could produce a batch of modules diverting votes to a given party. This would be a very expensive proposition and require a number of highly talented computer people. Doing this from within the manufacturing company seems unlikely. It would require that the ballot modules be manufactured using different chips, something that is highly unlikely to go unnoticed. Attacking them during shipping seems more viable, as there would be large numbers of them together. During programming, storage, transportation to the centres there are too few together and too many people would have to be involved. Because the modules are often tested, the modified modules would need to include a battery to run a real-time clock (so that they would only record fraudulent votes on voting day, not on testing day [this type of attack is known as an "Easter Egg" because it only shows up on the appointed day]). The battery, computer and memory would have to appear identical to the original modules. This would be very difficult and very expensive with current technology.

Denial of Service attacks on Ballot Modules are difficult to mount on a wide scale. Early attacks would be noticed during programming (when replacements could be obtained), and late attacks would either be on a small scale or involve too many people. Most of the attacks on the Voting Machine suffer from the same problems as those on the Ballot Modules. Someone would have to build some new chips and replace them in the Voting Machine. This is somewhat easier, inasmuch as the attacker need only replace or reprogram the EPROMs. It shares the same time problems however, as it must function correctly during testing, and only record fraudulent votes during the actual election.

A possible alternative to the clock is for the fraudulent programs to look for a known candidate who would only be listed during elections. Thus the program could look to see if "Joe Bloggs" was on the ballot, and only cheat if he was. If a voting test were run with the actual candidate list, this attack would be exposed.

Figure 4: Voting Machine

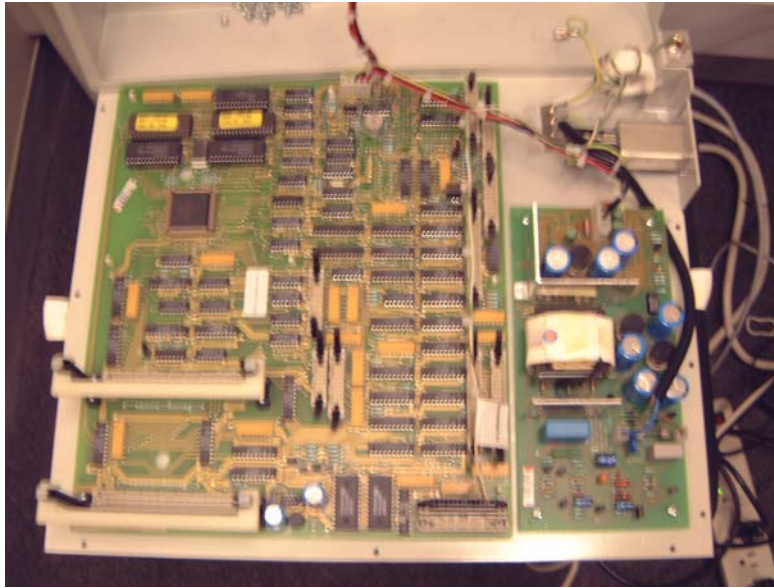


Fraudulent Count attacks on the IES software would involve running a hacked version of IES. The only times when the IES software is involved with the actual votes are during the reading of the Ballot Modules, the production of the CDs, and the counting of the votes. A hacked IES in the

Service Centre could report any votes the attacker desired. A hacked IES at the Local Level could count the votes any way the attacker desired. A variation of the IES attack would be to attack the host PC, so that it would run some alternate software. If the PC hardware that the IES is running on has been adequately safeguarded, it is possible to definitively prove that the IES software on it is the correct software; we can boot the PC from a CD and use programs on the CD to verify that the programs on the hard disk are correct. Denial of Service attacks on IES are also thwarted by verification.

Fraudulent Count attacks against the PRU involve substituting EPROMs, as in the Voting Machine attacks. They have the same problem of needing to report fraudulent results only in actual elections. Hence the need for a real-time clock or something else to identify actual elections. Because the Ballot Modules might be read separately, on a different PRU, it would be virtually impossible to avoid detection. Denial of Service attacks could be similarly discovered.

Figure 5: Insides of the PRU (the same boards are used in the Voting Machine)



The foregoing are the main technical components in the proposed voting system and the types of attacks that can be launched against them. Other, more specific attacks are all subject to the same set of requirements regarding what the attacks have to alter (EPROMS, CPUs, software), how many people have to be involved at the different levels to be effective, and what they have to do to avoid detection.

There are so many different kinds of attacks that are possible that, at first glance, it would seem impossible to adequately protect against all of them. Testing the machines before the election can find all but the attacks that add batteries and clocks to the voting machine. Parallel testing will detect even these problems. The basic idea behind parallel testing is that, on voting day, we select a random set of voting machines and run a parallel election on them – an election where we know what the input votes are. If they all produce the correct results, then we can be statistically certain that the machines have not been compromised. The quality of the test depends on the size and randomness of the sample of voting machines and test votes. While, for obvious reasons, we cannot conduct parallel testing as part of this report, we have conducted an extensive input-output test of the deployed voting machines that differs from a parallel test only in not being conducted on the

day of the election. The following section presents the results of that test. We then report the results of our tests of the system from the different perspectives of the election officials, the poll workers and the voters.

5 Input-Output test of voting machines

5.1 Objective

The objective of the input-output test was to determine whether the voting machines destined for use in the 2004 European and local elections can accurately record the preferences of the voters. It is conceivable that, either through malfunction or malicious interference, the voting machines could provide a distorted record of the votes that are entered on them. In short, our purpose is to provide evidence of the accuracy or otherwise of the deployed voting machines as devices for recording the votes of the people. The nub of the test is an input-output comparison of a representative sample of the almost 7,000 machines that have already been deployed around the country in preparation for the June 2004 elections. This test was implemented using a triple-lock verification of the vote input process as explained in Section 5.2 below. The test was carried out at 24 machine distribution centres throughout the country. Data were input and verified by teams of interviewers drawn from the ESRI's national panel of interviewers in collaboration with Returning Officers or their representatives in each centre. The research design proposed that a total of 37,500 votes would be input in this way. In addition to the main field experiment, a smaller parallel exercise was undertaken in the ESRI's offices in Dublin. This more limited experiment (involving the input of 5,000 votes on 5 voting machines) was videotaped throughout the three days it took to input the data. The purpose of the more controlled videotaped exercise was to enable us to definitively identify the source of any discrepancies between input and output that might arise and, in particular, to distinguish between machine and human error.

In Section 5.2 we describe the detail of the research design. Section 5.3 considers sampling issues. Section 5.4 discusses the preparation of test materials and the training of ESRI personnel. Section 5.5 describes the videotaped test of the input of 5,000 votes carried out in the ESRI's offices in Dublin. Section 5.6 presents the results of the two tests. Finally, Section 5.7 presents a summary and conclusions.

5.2 Experimental Design

In preparation for the test, the UCD/ESRI team prepared a simulated ballot for a notional national constituency with 12 candidates and randomly generated a set of more than 40,000 sets of preferences relating to the hypothetical candidates. For the main test, 750 voting machines were randomly selected across the 24 distribution centres. ESRI interviewers were instructed on how to enter 50 simulated ballot papers on each of the selected voting machines. These votes were recorded on ballot modules (devices somewhat similar to computer diskettes) inserted in the machines.

The data entry teams consisted of 3 persons – two interviewers from the ESRI's national panel and the Returning Officer for the area in question or his/her representative. Each of the 50 votes was entered by one of the ESRI interviewers. He/she then checked that the vote had been entered correctly. When satisfied that this was the case he/she signed the ballot paper and handed the booklet containing the relevant 50 ballot papers to the Returning Officer (or his/her representative). The Returning Officer in turn verified the vote and (when satisfied that it was correct) signed the

ballot paper. He/she then passed the booklet of ballot papers to the second ESRI interviewer who also checked the vote showing on the screen against the printed ballot paper and signed it when satisfied that it had been entered correctly. When all 3 had signed the relevant ballot paper the vote was cast by pressing the “Cast Vote” button on the machine. Each of the 50 simulated ballot papers in each booklet was entered onto a voting machine and verified in this way. The poll was then closed and the module removed and sealed in an envelope for return to the ESRI for analysis. This process was repeated for each of the machines in the final sample.

The scale of the current exercise should not be underestimated. In the main test, a total of 37,500 simulated ballots were issued by the research team for entry onto a random sample of voting machines over the course of 3 days in 24 different count centres throughout the country. This involved a total of 186,715 key presses³ on the voting machines to register each candidate preference plus the additional presses associated with the “cast vote” key for each ballot.

The triple-lock verification procedure outlined above was set up with a view to minimising the extent of human error in inputting the vote. It should be noted that the data-input task is much more onerous for the experimental data inputter than it is for an elector casting his/her vote on the day of the election. When casting a vote, one enters one’s preferences “directly” – from the mind to the machine. The design implemented for this input-output test required the “voter” to read the individual vote from the paper ballot and then enter the relevant preference pattern onto the machine. This was repeated 50 times per machine. The demands of this task give a whole new meaning to the term “voter fatigue”. Moreover, each preference set entered was randomly generated. It did not represent any party or other political allegiance held by the “voter” or follow any intelligible party pattern. In an actual election the typical voter is likely to have a single, clear set of voting preference in mind before entering the polling booth. This is not the case with the current experiment. In this regard the input-output experiment can be interpreted as imposing a substantially more stringent demand on the data inputters than that imposed on the voter on election day.

This brings us to the question as to whether or not one should expect errors in the input of the simulated ballots and, if so, what would be an “acceptable level” of any such errors. Unfortunately there is no readily available benchmark available. The absence of such a benchmark was a major factor in our decision to conduct the videotaped experiment to identify the extent and nature of input error in a controlled and videoed environment (see below).

5.3 Sampling

A total of 6,972 voting machines have been acquired for the forthcoming elections⁴. We initially selected a random sample of 750 of these machines (on a simple random selection basis). The ID numbers of each of the selected machines were sent to the relevant Returning Officer who was asked to locate the machines in question and have them ready for use by the ESRI interviewers on their arrival at the distribution centres. The acquisition of the specified machines proved substantially more difficult than anticipated. It seems that there were two main reasons for this. First, in some cases the machines had been sent away from the distribution centre for local use in training or demonstration. Secondly, given the physical shape and layout of the voting machines it is actually quite difficult to identify the ID number. Many of the distribution centres in question

³ The average number of votes per simulated ballot paper was 4.98.

⁴ It is our understanding that approximately 6,000 of these will be used on the day with approximately 1,000 machines being held in reserve as a contingency measure.

were large warehouses with substantial numbers of machines in storage. Under such circumstances it proved extremely difficult, if not impossible, for Returning Officers and their staff to provide the exact machines specified in the sample. Accordingly, although we attempted to secure a simple random sample of machines for testing purposes, only 57.4 per cent of the specified machines were actually made available to us. The deficit was made up by a selection made locally at the distribution centre by the Returning Officer. When the Returning Officer informed the ESRI that the specified randomly selected machines would not be available he/she was instructed on how to select every n^{th} machine from those in the distribution centre. Provided the Returning Officers followed the specified procedure, there should not be a problem in merging the sample of machines selected in this way (strictly speaking a systematic sample) with the original sample and treating the total sample as a random one. We are confident that the Returning Officers followed the selection instructions carefully and that this departure from pure randomness is unlikely to have introduced bias into the results. However, resource constraints in one distribution centre meant that it was only possible to make 33 rather than the target 44 machines available for data input. Accordingly, we were only able to test 739 machines instead of the 750 included in the original sample. Table 1 outlines the distribution of machines tested across the 24 machine storage/distribution centres.

Table 1: Number of machines tested in each distribution centre.

Centre	No.	Centre	No.	Centre	No.
Carlow	26	Galway	32	Meath	24
Cavan/Monaghan	27	Kerry	30	Roscommon	16
Clare	20	Kildare	26	Sligo/Leitrim	23
Cork City	44	Laois/Offaly	20	Tipperary	43
Cork County	33	Limerick	33	Waterford	18
Donegal	30	Longford	8	Westmeath	15
Dublin City	97	Louth	16	Wexford	23
Dublin County	83	Mayo	29	Wicklow	23
				Total	739

5.4 Preparation of the Test Materials and Interviewer Training

A single fictitious national constituency was set up with 12 candidates as follows:

Ahern – Fianna Fáil	Cullen – Fianna Fáil	Ó’Caoláin – Sinn Féin
Banotti – Fine Gael	Gregory – Non-Party	Rabbitte – The Labour Party
Burton – The Labour Party	Harney – Progressive Democrats	Sargent – Green Party
Coughlan – Fianna Fáil	Kenny – Fine Gael	Scallon – Non-Party

A ballot paper, corresponding to these candidates, was prepared using the IES software, and copies of this were printed on paper sized to fit on the voting machines⁵ (see Figure 6 below).

The randomly generated votes were prepared, printed and bound into booklets (one vote, i.e., one set of preferences per page). It is known that only a minority of voters utilise all the preferences available to them. The overall preference utilisation pattern of these randomly prepared votes was,

⁵ The ballots for this simulated constituency, which were used in the final test of the machines, were printed by the Department of the Environment, Heritage and Local Government.

therefore, constrained to match that of the 12-candidate constituency in Dublin North in the 2002 Dáil election⁶. This preference utilisation pattern is outlined in Table 2 below:

Table 2: Proportion stopping after allocating n^{th} preference

Preference	Per Cent Stopping	Preference	Per Cent Stopping
1	3.9	7	5.0
2	6.4	8	3.0
3	28.6	9	1.6
4	17.9	10	1.5
5	14.0	11	1.4
6	8.4	12	8.3
		Total	100.0

Each group of 50 ballots was prepared as a single booklet. Each booklet was entered onto a different voting machine and ballot module.

All ESRI interviewers involved in the test attended a half-day training session in the ESRI's offices in Dublin on either Thursday 15th or Friday 16th April. This involved a group instruction session followed by "hands-on" experience with the machines. The group instruction session dealt with the background to the test; the ballot papers; an overview of the voting machines and ballot modules and also detailed instruction on all operational aspects of the test. This latter involved providing all interviewers with direct access to voting machines and bringing them through all operational stages of the experiment⁷.

A system of unique ID numbers was used to relate the booklet of simulated ballot papers to the module, voting machine and till receipt from the voting machine. On completion of each booklet of ballots the signed booklet, ballot module and till receipt (the written record produced by the voting machine at the end of input) were sealed in an envelope which was then returned to the ESRI offices for analysis.

5.5 The Parallel Videotaped Experiment

In addition to the general entry of the 36,950 simulated ballots a further aspect of the study design involved the entry of 5,000 ballots under controlled videotaped conditions in the ESRI's offices in Dublin. The 5,000 simulated votes were contained in 100 booklets of 50 votes. The votes were input under conditions comparable to those used throughout the 24 distribution centres. The principal difference between this test and the main test at the 24 distribution centres was that the entry of ballots in the ESRI's offices was videotaped. The purpose of this experiment was to provide the research team with a better understanding of any errors that might crop up. In the event of any such errors occurring, we were conscious that it would be difficult to distinguish between genuine (unobserved) data input errors on the one hand and machine errors on the other. The videotaped experiment was built into the design in order to address this issue. If errors became

⁶ See Sinnott, R., and McBride, J. (2004), 'Preference utilisation in three electronic voting constituencies in the 2002 Dáil election', POPB Working Paper 2004/01, Dublin.

⁷ Six voting machines, 6 programming/reading units and approximately 970 voting modules were made available by the Commission to the UCD/ESRI team to carry out the experiment. We wish to thank Mr. David Walsh from the Department of the Environment, Heritage and Local Government for facilitating the provision of the machines and for assistance with the software.

apparent in the main phase of data entry one could assume that they would also appear, even if perhaps at a lower rate, in the more controlled video-taped test. Where input-output inconsistencies appeared in the latter we would be able to review the videotape and definitively say whether or not the inconsistency between observed and expected ballot was due to an input error or due to a machine error⁸.

5.6 Results

Initial Findings

As noted above, 739 machines were tested in the field. Accordingly, a total of 36,950 ballots should have been cast and recorded (50 on each machine). We term these the “target votes”. The core of the test procedure consists of comparing these target votes on a vote-by-vote basis with the votes actually recorded on the modules from the machines, which we call the “cast votes”. The recorded votes were copied from the modules using the dedicated software and the programming-reading units supplied by the Commission. These were then transferred to the ESRI’s computer system. An aggregated file of votes cast was set up. This file was compared with the file of target votes which had been randomly generated by the UCD/ESRI team. Independent comparisons were made using both ACCESS and SPSS software. This approach was used for both the main set of votes from the field experiment and also for the votes that were entered with video recording of the vote-entry process at the ESRI.

The numerical relationship between the two sets of votes is shown in Table 3. When all data entry was completed, the first step was to count the total number of cast votes on all the modules. A total of 36,934 were found, i.e. the modules appeared to be 16 votes short of the expected total. Examination of the individual modules showed, however, that 22 modules were short one vote, i.e. recorded only 49 instead of 50 votes and a further six modules contained an “extra” vote, i.e. contained 51 votes instead of the expected 50. Thus, the net shortage of 16 votes was composed of 22 “missing” votes and 6 “extra” votes.

Table 3: Relationship between Target Votes and Cast Votes

Total target votes issued (=739 booklets of 50 ballots each)	36,950	100.000%
Total cast votes (= votes recorded on the modules)	36,934	99.957%
Votes perfectly recorded (=cast votes corresponding perfectly with target votes)	36,831	99.678%
"Extra" votes (=modules with 51 votes recorded)	6	0.016%
Missing votes (=modules with 49 votes recorded)	22	0.060%
Aberrant votes (=cast votes not corresponding exactly with target votes)	97	0.263%

⁸ It should be noted that there was at least one significant operational difference between the implementation of the test as conducted in the machine distribution centres and that carried out in the ESRI’s offices. As noted above, in the machine distribution centres the input team was made up of two ESRI data inputters plus the Returning Officer or his/her representative(s). In the videotaped experiment conducted in the ESRI’s offices Returning Officers were not available. Their place was taken by a third ESRI interviewer or other staff member who was trained by the project team to take the role of the Returning Officer. All ESRI interviewers who participated in the videotaped experiment at the ESRI’s offices participated in the more general experiment at the machine distribution centres.

The next step was to compare the target votes with the cast votes on a vote-by-vote basis. This showed that 36,831 or 99.68% of the 36,950 target votes given to the teams for input into the machines duly turned up as votes correctly recorded on the ballot modules. This level of accuracy in the input and recording of votes is sufficient to rule out any sustained fraud or machine error.

However, 119 or 0.32% of the votes given to the input teams for entry on the machines did not turn up in the output, this total comprising the 22 missing votes plus the 97 aberrant votes. A further 6 votes (0.02%) were cast which should not have appeared on the modules. Our focus now turns to the nature of these errors, the key question being whether the discrepancies in question were due to machine error in the recording of votes or to human error in the input process. In order to understand how the discrepancies might have arisen, we begin by examining the results of the videotaped input experiment.

Evidence from the Video Recorded Experiment

In the videoed experiment, 5,000 votes were entered onto 5 voting machines. The results showed that, even in a highly controlled, almost laboratory environment, with tight monitoring and videotaping, a total of 5 errors occurred in the process of input/recording of the votes on the modules⁹. When the video-tapes of the input of the five votes in question were replayed, the evidence was conclusive – the 5 errors were due entirely to human error in the data entry process. The error patterns from the videotaped experiment are outlined in Table 4, which shows that the discrepancies were due to human errors of the following kinds:

- omission of a last preference on a ballot paper as in the first case listed in Table 4 (Module 882, Ballot 30);
- vertical displacement of a preference or transposition of a pair of preferences. This would occur where the data inputter transposes the preferences assigned to two neighbouring candidates as he or she is transferring the vote from the printed simulated ballot paper on to the electronic voting machine¹⁰. There are three examples of this in Table 4, namely the second, third and fourth cases listed (Module 828, Ballot 35; Module 887 Ballot 20; Module 894 Ballot 6);
- the remaining case in Table 4 is more complex as it involves omission of the preference for one candidate and transposition of the preferences for another two. This leads to the casting of a preference set which is quite different to that intended (see the fifth case listed (Module 895 Ballot 1) in Table 4).

⁹ The error rate of 1 in 1,000 in the videotaped experiment compares with approximately 3 in 1,000 of the votes entered in the main experiment. This is consistent with clear evidence from other disciplines that the simple act of being studied itself causes improved performance on the part of subjects. This is the so-called Hawthorne Effect and is, in our view, responsible for the lower overall error rates recorded in the videotaped experiment.

¹⁰ Evidence of similar vertical proximity effects has been documented in Sled, S (2003), 'Vertical proximity effects in the California recall election', Caltech/MIT Voting Technology Project Working Paper, Pasadena/Cambridge.

Table 4: Error patterns from the videotaped experiment.

Module Number	Ballot Number	Preference set of target vote	Preference set of cast vote	Type of Error
882	30	00010002000 <u>3</u>	00010002000 <u>0</u>	Omission of last preference
828	35	30100000 <u>02</u> 00	30100000 <u>20</u> 00	Transposition of 2 adjacent preferences
887	20	20500 <u>06</u> 34100	20500 <u>60</u> 34100	Transposition of 2 adjacent preferences
894	6	00 <u>60</u> 05431020	00 <u>06</u> 05431020	Transposition of 2 adjacent preferences
895	1	<u>2</u> 0000 <u>1030</u> 000	<u>10000000</u> <u>2</u> 000	Combined omission and transposition

- In addition to the five discrepant votes just considered, we found that on one module in the video experiment only 49 votes were registered. The omitted vote (on module 857) was the 50th simulated ballot in the booklet. The vote preference was 350241000000 in order from candidate 1 to candidate 12. It is clear from the videotape that the vote was entered correctly. It appears, however, that the relevant data entry operator omitted to actually cast the vote as the video shows no attempt to press the cast vote button on the voting machine.

Obviously, one cannot assume that, simply because we can show that the six errors in the 5,000 votes entered in the video experiment were due to human error, all the errors that occurred in the field work were also attributable to human error. Nonetheless, the video evidence performs a vitally important function in demonstrating that, even given the triple check procedure, human error does occur in a data input process like this. The video evidence is also vital in giving an indication of the kinds of errors that are likely to occur.

The Nature of the Discrepancies in the Main Sample

With this evidence in mind, we can now examine the discrepancies in the main sample. In Table 3 above, three main types of error were identified:

1. “Extra” votes:

There were 6 “extra” votes (i.e. 6 modules contained 51 votes) and these are shown in full in Table 5. The “Comment” column of the Table gives an explanation of how the error is likely to have occurred. The first ballot contains a pattern of preferences running 1 to 12¹¹, in order of the candidates on the ballot paper. There was no such ballot in the 36,950 target votes issued. The most plausible explanation is that this extra vote was due to data entry operators experimenting with their first machine and inadvertently casting a vote running 1 to 12 in sequence. The second ballot listed, from module 10, is an exact duplicate of ballot 9 in the same module, i.e. it appears that ballot 9 was inadvertently entered twice. In all of the other four cases, the operators realised they had made an error and noted this on the booklet at the time of entry. These consisted of three cases where a ballot was entered twice and one case

¹¹ Note that a code ‘A’ signifies a preference 10; ‘B’ a preference 11 and ‘C’ a preference 12. All votes were, of course, entered in pure numeric form in all parts of the experiment.

where a ballot with a single preference in the last position (which did not exist in the target set) was erroneously entered and the problem noted in the booklet.

Table 5: “Extra” votes on the 6 modules containing 51 votes.

Module Number	Cast Vote	Comment
2	123456789ABC	See explanation in the text above.
10	100020300000	Ballot 9 entered twice. No note on booklet
126	056327000401	Problem noted on booklet. Ballot 42 entered twice
127	000040325001	Problem noted on booklet. Ballot 50 entered twice
128	000000000001	Problem noted on booklet. Cast in error at ballot 9
130	400102305000	Problem noted on booklet. Ballot 49 entered twice

2. “Missing” votes:

It was shown above that there were 22 missing votes (i.e. 22 modules contained only 49 votes instead of 50). Table 6 gives the full detail of these votes and a comment as to how the problem appears to have arisen. In three cases the ballot in the booklet was not signed and clearly was not entered. In 4 further cases, there was a note on the booklet to say that the data entry operators realised that they had failed to enter the ballot. In the other 15 cases, we believe that the most likely explanation is that, as with the missing vote in the videotaped experiment, the “Cast Vote” button was not properly activated by the operators.

Table 6: Full listing of Missing Votes - modules on which only 49 votes registered.

A	B	C	D	E
	Module	Ballot	Target Vote	Comment
1	26	28	010432500000	Ballot in booklet not signed – page obviously missed
2	41	48	010000002030	
3	83	31	035001260040	Note on booklet - realised failed to enter ballot
4	149	50	005460230100	Note on booklet - realised failed to enter ballot
5	254	14	260413000500	Ballot in booklet not signed – page obviously missed
6	273	7	020000100300	Ballot in booklet not signed – page obviously missed
7	305	50	000200013040	Note on booklet - realised failed to enter ballot
8	317	50	701530046200	
9	327	50	200100000300	
10	336	20	050243010000	
11	337	40	000010423000	
12	447	50	701280036054	
13	457	37	000030002010	Note on booklet - realised failed to enter ballot
14	463	50	010003020000	
15	501	50	100000003002	
16	530	42	000000000100	
17	537	48	000100230000	
18	553	50	000000010200	
19	573	11	010000000000	
20	595	12	B8763512C9A4	
21	607	48	012004605370	
22	640	50	000000210000	Note on booklet - realised failed to enter ballot

Note: A code of 'A' in preference pattern signifies a 10th preference; 'B' signifies an 11th. preference and 'C' signifies a 12th. preference.

3. “Aberrant” votes:

These were the 97 cases in which a target vote and a cast vote existed, but the correspondence between the two was not exact. Table 7 lists all 97 cases in full. The data in Table 7 make it possible to conduct a vote by vote analysis of the 97 discrepancies. A summary analysis of the error patterns identified is given in Table 8.

The Error Patterns in the Aberrant Votes

One complication must be noted at the outset. The complication arises in comparing the cast votes to the target votes. To protect the anonymity of the elector and the secrecy of the ballot, the votes that are cast on a module are stored in a randomised order. Consequently, it is not possible to identify a recorded vote as being the 1st., 2nd., 3rd. ... 50th vote cast. In matching votes cast with those target votes one must rely on the matching of preference patterns within ballot modules between the set of generated votes and those actually cast on the day as part of the experiment.¹²

Table 7 lists each of the discrepancies between target votes and cast votes. Column A simply contains a sequence number from 1 to 97. Column B contains the module number (or booklet number) in which the discrepancy arose and Column C indicates the ballot number of that vote within the booklet. Column D specifies the vote that should have been cast, i.e. the preference set of the 'target' vote as generated by the research team. Column E lists the cast votes that were aberrant (in the sense that they differed to some extent from the target set generated by the research team). Column F classifies the error into a number of basic categories and Column G identifies any special features of the vote in question.

We now indicate how each aberrant vote can be reconciled or matched with the corresponding target vote on the basis of relatively simple and intelligible error patterns. Consider the first row of Table 7. This shows that in module number 1, ballot number 15 we had a target vote 034560810720. This vote should have been cast but which was not registered on module No 1. However, on that same module we had a vote cast as 034560010720. This vote appears to have been cast in error. When the two votes are placed one on top of the other as below it is clear that the problem is an omission of the 8th preference on the vote actually cast:

<i>Module 1</i>	<i>Ballot paper 15:</i>
Target Vote	034560 <u>8</u> 10720
Actual Vote	034560 <u>0</u> 10720

Accordingly, we have classified the above as an omission of last preference. A different data entry error is apparent, for example, from module 15, ballot paper No. 1. In this case we have the straight transposition of the preferences for the second and third candidates.

<i>Module 15</i>	<i>Ballot paper 1:</i>
Target Vote	<u>06</u> 040530012
Actual Vote	<u>006</u> 040530012

One can see that in the 'target' vote Candidate 2 should have been given a preference '6' and Candidate 3 a preference of '0'. On the vote that was actually cast Candidate 2 was assigned a '0'

¹² There is an option in the counting software to mix and randomise votes *between* modules. This option can be turned off – so allowing our test to take place. One cannot, however, turn off the mixing *within* module.

and Candidate 3 assigned a preference of '6'. This represents a simple transposition or a form of vertical displacement as it appeared on the voting machine.

A slightly more complex form of data entry error combines both omission and transposition. Consider, for example, line 17, module 117 ballot 6 in Table 7. In this ballot the data entry operation omitted to enter the 2nd preference for the sixth candidate on the ballot paper and instead assigned a 2nd preference to the second candidate (who should, in fact, have been given a third preference).

Module 117 Ballot paper 6:
 Target Vote 130002000000
 Actual Vote 120000000000

Table 7: Detailed description of nature of inconsistencies between 'target' and 'cast' votes

A	B	C	D	E	F
	Module	Ballot	Target Vote	Cast Vote	Type of Error
1	1	15	034560810720	034560010720	Omission of last preference
2	1	21	627108000345	627100000345	Omission of last preference
3	4	12	030201400000	032001400000	Single transposition of 2 adjacent votes
4	11	28	000023001000	000012003000	Combined omission and transposition
5	13	24	206405000103	200405000103	Omission of last preference
6	15	1	060040530012	006040530012	Single transposition of 2 adjacent votes
7	15	24	000302001000	300002000100	Transposition of 2 non-adjacent votes
8	15	25	004500200103	004502001003	Combined omission and transposition
9	16	36	023000010000	002000010000	Combined omission and transposition
10	24	30	743095120608	743005120608	Omission of last preference
11	59	37	100000000000	130004206005	Combined omission and transposition ¹³
12	67	1	000100354620	700100354620	Omission of last preference
13	104	3	002010000003	020010000003	Single transposition of 2 adjacent votes
14	107	35	200000100300	200000100030	Single transposition of 2 adjacent votes
15	108	5	023156040000	023105640000	Combined omission and transposition
16	113	36	010200000000	310200000000	Omission of last preference
17	117	6	130002000000	120000000000	Combined omission and transposition
18	123	47	020000000100	020000000010	Single transposition of 2 adjacent votes
19	124	50	300040002001	200030001000	Combined omission and transposition
20	127	41	000004320010	000004320100	Single transposition of 2 adjacent votes
21	136	46	502640003010	502640003001	Single transposition of 2 adjacent votes
22	137	28	002010003045	002001003045	Single transposition of 2 adjacent votes
23	167	28	102005004003	102000004003	Omission of last preference
24	170	18	020140300000	020140350000	Omission of last preference
25	170	42	002516400030	002010000000	Combined omission and transposition ¹⁴
26	170	50	062103450000	062103450070	Omission of last preference
27	175	10	000302100000	000302100004	Additional last preference cast
28	183	21	000000000001	102050003004	Combined omission and transposition ¹⁵
29	185	5	030000001020	003000001020	Single transposition of 2 adjacent votes
30	186	42	300000000102	000000000102	Omission of last preference
31	187	8	300162700045	301062700045	Single transposition of 2 adjacent votes
32	187	17	140200003000	104200003000	Single transposition of 2 adjacent votes
33	189	4	003410265000	003401265000	Single transposition of 2 adjacent votes
34	189	19	310078206045	301078206045	Single transposition of 2 adjacent votes
35	190	45	403020000010	400320000010	Single transposition of 2 adjacent votes

¹³ See note A below

¹⁴ See note B below

¹⁵ Note on booklet - ballot 24 cast twice; 21 not cast

A	B	C	D	E	F
	Module	Ballot	Target Vote	Cast Vote	Type of Error
36	192	4	00043 <u>6</u> 000215	00043 <u>0</u> 000215	Omission of last preference
37	192	20	<u>2</u> 630 <u>0</u> 0007514	<u>2</u> 030 <u>6</u> 0007514	Transposition of 2 non-adjacent votes
38	192	33	0102 <u>5</u> 3000004	0102 <u>0</u> 3000004	Omission of last preference
39	249	38	310200 <u>5</u> 00400	310200 <u>0</u> 00400	Omission of last preference
40	250	26	0300 <u>4</u> 0020 <u>5</u> 01	0300 <u>0</u> 0020 <u>0</u> 01	Combined omission and transposition
41	252	31	<u>1</u> 0000 <u>3</u> 000 <u>2</u> 00	<u>0</u> 0000 <u>2</u> 000 <u>1</u> 00	Combined omission and transposition
42	254	4	<u>0</u> 0100000 <u>2</u> 00	<u>1</u> 0000000 <u>0</u> 00	Combined omission and transposition
43	257	6	00000 <u>3</u> 200100	00000 <u>2</u> 300100	Single transposition of 2 adjacent votes
44	259	45	000423000 <u>1</u> 00	000423000 <u>0</u> 10	Single transposition of 2 adjacent votes
45	278	31	0020000 <u>3</u> 0100	00 <u>3</u> 0000 <u>2</u> 0100	Transposition of 2 non-adjacent votes
46	286	36	0000 <u>3</u> 01 <u>2</u> 0000	0000 <u>0</u> 21 <u>3</u> 0000	Combined omission and transposition ¹⁶
47	300	42	<u>0</u> 3000 <u>1</u> 0000 <u>2</u>	<u>0</u> 2000 <u>0</u> 0000 <u>1</u>	Combined omission and transposition
48	303	22	000003000 <u>0</u> 102	00000300 <u>1</u> 002	Single transposition of 2 adjacent votes
49	311	8	02463 <u>8</u> 071050	02463 <u>0</u> 071050	Omission of last preference
50	311	16	2135000 <u>7</u> 0460	2135000 <u>0</u> 0460	Omission of last preference
51	322	12	0001 <u>0</u> 2000340	0001 <u>2</u> 0000340	Single transposition of 2 adjacent votes
52	330	45	000 <u>0</u> 30200041	000 <u>3</u> 00200041	Single transposition of 2 adjacent votes
53	338	21	5803 <u>9</u> 2701460	5803 <u>0</u> 2701460	Omission of last preference
54	340	37	<u>2</u> 07103065040	<u>2</u> 00103065040	Omission of last preference
55	369	3	<u>0</u> 0 <u>7</u> 0263 <u>8</u> 415	<u>0</u> 7 <u>0</u> 00263 <u>0</u> 415	Combined omission and transposition
56	386	35	0020140000 <u>3</u> 0	0020140000 <u>0</u> 3	Single transposition of 2 adjacent votes
57	434	8	<u>0</u> 0 <u>1</u> 32540000	<u>0</u> 0 <u>4</u> 103002000	Combined omission and transposition ¹⁷
58	449	2	001024005 <u>0</u> 63	001024005 <u>6</u> 03	Single transposition of 2 adjacent votes
59	451	34	<u>3</u> 02000 <u>0</u> 1000	<u>0</u> 2000 <u>3</u> 01000	Transposition of 2 non-adjacent votes
60	463	43	302000 <u>0</u> 10000	302000 <u>1</u> 00000	Single transposition of 2 adjacent votes
61	479	13	000 <u>0</u> 10200003	000 <u>1</u> 00200003	Single transposition of 2 adjacent votes
62	482	20	000 <u>0</u> 23401000	000 <u>2</u> 3401000	Combined omission and transposition
63	489	20	107026304005	100026304005	Omission of last preference
64	494	25	<u>0</u> 1034000020	<u>0</u> 10034000020	Single transposition of 2 adjacent votes
65	496	40	00100000 <u>5</u> 4 <u>2</u> 3	00100000 <u>4</u> 3 <u>2</u> 0	Combined omission and transposition
66	499	11	00300000 <u>2</u> 001	00300000 <u>0</u> 201	Single transposition of 2 adjacent votes
67	501	25	<u>0</u> 20100000000	<u>0</u> 21000000000	Single transposition of 2 adjacent votes ¹⁸
68	512	7	001700625 <u>8</u> 34	001700625 <u>0</u> 34	Omission of last preference
69	513	39	30000 <u>5</u> 002014	30000 <u>0</u> 002014	Omission of last preference
70	515	40	0010000000 <u>0</u>	00100 <u>3</u> 20000 <u>4</u>	Combined omission and transposition ¹⁹
71	517	30	20310040 <u>0</u> 0 <u>5</u> 0	20310040 <u>5</u> 0 <u>0</u>	Transposition of 2 non-adjacent votes
72	522	27	20130600 <u>4</u> 500	20130600 <u>5</u> 400	Single transposition of 2 adjacent votes
73	522	35	54020 <u>6</u> 000130	540200000130	Omission of last preference ²⁰
74	525	5	000 <u>1</u> 00 <u>3</u> 20400	00000 <u>2</u> 10 <u>3</u> 00	Combined omission and transposition
75	531	20	0300010000 <u>2</u> 0	0300010000 <u>0</u> 2	Single transposition of 2 adjacent votes
76	531	28	0040020300 <u>1</u> 0	0040020300 <u>0</u> 1	Single transposition of 2 adjacent votes
77	546	16	04 <u>9</u> 80261753	04 <u>0</u> 80261753	Single transposition of 2 adjacent votes
78	550	17	<u>5</u> 00000 <u>3</u> 200 <u>4</u> 1	<u>4</u> 00000 <u>2</u> 100 <u>3</u> 0	Combined omission and transposition
79	550	49	004516382 <u>A</u> 79	004516382 <u>0</u> 79	Omission of last preference
80	553	10	0043 <u>8</u> 0271056	0043 <u>0</u> 0271056	Omission of last preference
81	587	10	<u>3</u> 04000100200	<u>3</u> 40000100200	Single transposition of 2 adjacent votes
82	598	38	0062 <u>7</u> 3104050	0062 <u>0</u> 3104050	Omission of last preference
83	609	6	<u>0</u> 50030001 <u>4</u> 02	<u>0</u> 40030001 <u>0</u> 02	Combined omission and transposition
84	610	32	304060 <u>7</u> 12005	304060 <u>0</u> 12005	Omission of last preference
85	610	39	<u>0</u> 1 <u>2</u> 300500040	<u>0</u> 1 <u>2</u> 300500040	Combined omission and transposition
86	611	31	60451000 <u>3</u> 200	60451000 <u>0</u> 320	Combined omission and transposition

¹⁶ Note on booklet re. entering wrong sequence

¹⁷ Note on booklet - ballot 9 cast twice; 8 not cast

¹⁸ Note on booklet - possible error on entered ballot

¹⁹ Note on booklet - error on entered ballot

²⁰ Note on booklet - realised failed to enter preference 6

A	B	C	D	E	F
	Module	Ballot	Target Vote	Cast Vote	Type of Error
87	611	48	010000 5 42030	010000 5 042030	Single transposition of 2 adjacent votes
88	612	46	3 01000 6 502040	0 01000 5 402030	Combined omission and transposition
89	662	1	000 3 00004201	00 3 000004201	Single transposition of 2 adjacent votes
90	662	41	000 2 00001003	00 2 000001003	Single transposition of 2 adjacent votes
91	663	10	60543 8 012007	60543 0 012007	Omission of last preference
92	674	25	300000200 1 00	30000020 1 000	Single transposition of 2 adjacent votes
93	682	16	000 1 03020000	00 1 003020000	Single transposition of 2 adjacent votes
94	711	2	00 3 200100000	00 0 320100000	Combined omission and transposition
95	714	15	00 2 000145300	0 2 0000145300	Single transposition of 2 adjacent votes
96	714	27	8 0270450 6 013	0 01420300000	Combined omission and transposition ²¹
97	717	24	1 0000000 2 000	0 0000000 1 000	Combined omission and transposition ²²

Notes:

A: This data entry error appears to have been brought about by combining ballots 36 and 37 in booklet 59.
 B: This error pattern is consistent with the operator inadvertently pressing the button for the third preference a second time, thus cancelling the 3rd and subsequent preferences.
 A code of 'A' in a preference pattern signifies a 10th preference; 'B' signifies an 11th preference and 'C' signifies a 12th preference.

Detailed examination of the entire set of aberrant votes showed that *all* of them exhibited patterns of error entirely consistent with human error during the input process. The main types of error found in these votes are summarised in Table 8. Thus, some 27 per cent of the aberrant votes were explicable as omissions of the last preference on the ballot paper. About 43 per cent were due to vertical transposition of votes, almost always of adjacent votes. Approximately, 29 per cent of the discrepancies were due to more complex but still intelligible error patterns involving both omission and transposition.

Table 8: Distribution of aberrant votes by error type

Nature of error	No.of Votes	Per Cent
Omission of last preference	26	26.8
Additional last preference cast	1	1.0
Single transposition of 2 adjacent votes	37	38.1
Transposition of 2 non-adjacent votes	5	5.1
Combined omission and transposition	28	28.9
	97	100.0

5.7 Conclusion

Much of the above discussion focussed on the discrepancies encountered, their number, pattern and likely origin. However, it should be recalled that the machines recorded 99.68 per cent of the votes issued accurately. This indicates that there was no credible evidence of fraud or substantial machine failure.

However, despite the care we took in training and planning, and the triple check on data entry, there was an appreciable level of error. This took a number of forms – votes omitted which should have been entered, extra votes appearing which were not in the target set and erroneous entries. On

²¹ Note on booklet - ballot 27 missed, 26 entered twice
²² Note on booklet - ballot entered incorrectly

detailed examination, all of these errors appear much more likely to have arisen from mistakes by the operators as they entered the preferences than from any other sources. Video evidence lends further support to this view by showing that even in the very carefully controlled video-taped experiment all six discrepancies arising were attributable to human error.

Our analysis of the errors arising suggests topics that deserve attention in educating voters, training election staff, and in evaluating the usability of the machine. For example, the number of missing votes (22 modules with only 49 votes) where the last vote on the ballot was omitted raises the possibility that there may be a problem in the closing off procedures at the end of the voting process. Where possible, we address such usability problems in the remaining sections of this report.

On balance, however, we conclude that the voting machines deployed for use in the June 2004 European and Local elections appear to be a reliable means of recording the votes cast by the voters.

6 Using IES from the Local Electoral Area/ Constituency Worker's Perspective

The Local Electoral Area /constituency worker uses the IES to create a new "poll" object (we shall refer to this as a "race" as it consists of the information for a set of candidates who are all competing for a given set of seats). He or she enters information about the race (location, date, etc.) and enters the candidates' details from a form along with a picture on a CD. Once all the candidates' details are in, the official burns a CD with the information and sends it to the Service Centre. After the election, the Service Centre will send a CD with the full list of all the votes for that area back to the local centre. The workers load that CD and execute the count.

The operation of the software at this stage is fairly complicated. The workers at this level will probably have a moderate amount of training, but not a great deal of experience. This is something they will rarely do. There are a number of minor bugs, and there are several points in the process where mistakes are easy to make²³. Here are the issues we are concerned about:

- The "Close" button behaves inconsistently in different windows. It completes and finishes some tasks (indicated with a green checkmark), aborts others (indicated with a red "X"), appears to complete still others (green checkmark), but actually doesn't. Most of this is done without feedback.
- In some scrolling lists, an item is selected and processed by a double click. In others, one has to select the item first and then push an execution button.
- Keyboard accelerators (keystrokes that can be used in place of clicking the mouse) are confusing in many places. Many times the same keystroke is assigned to two different buttons ("cancel" and "complete" were both assigned Alt-C).



































²³ In case of PC setup problems, there is a service telephone number affixed to the top of the computer. The operator at "Sord Data Systems" we spoke to was quite knowledgeable.

- Delete key didn't work in all user interfaces but Backspace did.
- Scrolling in the help window only scrolls the page after release of the cursor button.
- Changing the date to the 99th day of December is possible in the text-formatted version of the date. This will not cause any problems until the data is written out to a file and sent to the Service Level, where it will mysteriously fail to load.
- In different places in the software, we have seen dates printed out as "6/11/2004", "11/06/2004", and "11/ 6/2004". (One of the machines we were running on was set to the "American" local, hence the Month/Day/Year. Dates should be consistent even if an Irish operator selects the "American" local.)
- The IES will allow the local level worker to enter impossibly large numbers of candidates (we entered 97). Only during the ballot layout procedure will it complain with the rather confusing error message "43 buttons. Incorrect manual selection of ballot papers columns".
- The "Double Height" option introduces one more bit of complexity into the system. Voters might find ballots made this way confusing. This is especially likely should one ballot paper be single height, while the next is double.
- The information surrounding the "database" and "securing the database" is vague. It is possible to "Secure the database" numerous times without any apparent effect.

Figure 6: A ballot paper

Column on Voting machine 2
size 126.8 x 465 mm

**TOGHCHÁN DO PHARLIAMINT NA HEORPA
TOGLACH BAILE ÁTHA CLIATH
EUROPEAN PARLIAMENT ELECTION
DUBLIN CONSTITUENCY**

	AHERN - FIANNA FÁIL Union of Europe of the Nations [UEN] (BERTIE AHERN) Liosta Ionad FF Replacement List		
	BANOTTI - FINE GAEL European People's Party (CD) & European Democrats [EPP-ED] (MARY BANOTTI) Liosta Ionad FG Replacement List		
	BURTON - THE LABOUR PARTY Party of European Socialists [PES] (JOAN BURTON) Liosta Ionad LAB Replacement List		
	COUGHLAN - FIANNA FÁIL Union of Europe of the Nations [UEN] (MARY COUGHLAN) Liosta Ionad FF Replacement List		
	CULLEN - FIANNA FÁIL Union of Europe of the Nations [UEN] (MARTIN CULLEN) Liosta Ionad FF Replacement List		
	GREGORY - NON-PARTY (TONY GREGORY) Liosta Ionad Non-P Replacement List		
	HARNEY - PROGRESSIVE DEMOCRATS (MARY HARNEY) Liosta Ionad PD Replacement List		
	KENNY - FINE GAEL European People's Party (CD) & European Democrats [EPP-ED] (ENDA KENNY) Liosta Ionad FG Replacement List		
	Ó'CAOLÁIN - SINN FÉIN (CAOIMHGHÍN Ó'CAOLÁIN) Liosta Ionad SF Replacement List		
	RABBITTE - THE LABOUR PARTY Party of European Socialists [PES] (PAT RABBITTE) Liosta Ionad LAB Replacement List		
	SARGENT - GREEN PARTY - COMHAONTAS GLAS Green Group (TREVOR SARGENT) Liosta Ionad GP/CG Replacement List		
	SCALLON - NON-PARTY (DANA ROSEMARY SCALLON) Liosta Ionad Non-P Replacement List		

- There is no connection between the picture to be printed on the ballot paper and the details for the person in question. It would be quite easy (and will almost certainly occur) for Ian Fleming's picture to be printed next to Ian Fitzgerald's name.
- "Delete Poll" is irreversible.
- The manual does not discuss the drawing of lots. When a lot-drawing situation arises, IES displays a popup window with no explanation of what to do.

6.1 Critical requirement

- All personnel using the IES system must demonstrate proficiency in hands-on, timed tests before using it to create or process elections (if it takes someone an hour to do what should take ten minutes, that is a problem).

6.2 Recommendations

- Deleted polls should be kept in a "Trash Can" in the same way as deleted files in most software applications.
- There should be some way of ensuring that the correct picture is associated with the correct candidate.
- "Securing the database" should not be a separate menu item. It should happen automatically when all the data have been read in. (There may be reasons that we are unaware of why securing the database must be done manually. At a minimum, it should be impossible to secure the database a second time.)
- All of the buttons, keyboard accelerators, selection mechanisms, etc. should behave in a uniform fashion.
- There should be only one way to change the date and it should be unambiguous. Because IES allows both Month/Day/Year and Day/Month/Year, the month should always be spelled out in all printouts and tools.
- The "Double Height" option should be eliminated.
- All menu items not required for the current operation should be disabled and greyed out.
- IES should not allow the operator to enter illegal data (e.g., 97 candidates).

7 Using IES from the Service Centre Worker's Perspective

The Service Centre worker uses the IES to create a new "poll" object (different from the "poll" object we called "race" above – we'll call this an "election" object). He/she then enters information about the election (date, polling stations to be used, etc.) and downloads the candidates' details from the CD received. When all the CDs from all the local levels are loaded, the worker will download

the information onto the Ballot Modules. The Ballot Modules will then be sent back to the local levels to be loaded into the Voting Machines.

When the election is over, the local levels will send the Ballot Modules back to the Service Centre. They will be read into the Service Centre's PC and a CD with the complete contents of the appropriate Ballot Modules will be created. The CD will be sent to the local levels for counting.

The operation of the software is fairly complicated. The workers at this level will probably have a lot of training and they will be working with the system often. There are a number of minor bugs, and there are several points in the process where mistakes are easy to make. In addition to the issues noted above, here are the things we are concerned about:

- The IES program that is run at the service level is exactly the same program as is run at the local level. Many inappropriate functions are enabled. For example, the "Candidate Details" dialog boxes allow the service level worker to change/add candidate information, even though that should only be done by the local level personnel.
- When a Ballot Module is in the Programming/Reading Unit, the operator cannot see the label to know which polling station the Ballot Module is intended for.
- Warnings regarding conditions under which the software might be vulnerable were not called out (e.g., the PC is connected to Internet, it is running with old versions; it is connected to a modem).
- The system of erasing ballot modules is ad-hoc. They are erased by default when programming new polls. There should be checks on this process.
- The "results file" contains the details of a race, including which ballot modules are needed to count the election. It is an XML file that we were able to modify in WordPad. The name "results file" is a misleading name for the file containing the details of a race.

7.1 Critical Requirements

- The results file must be backed up on two disks when created, one stored off site. It is further critical that it is authenticated when it is about to be used.
- The label for the ballot modules should extend over the "top" of the ballot module, so that it acts as a seal and so that the identification of the designated polling station is obvious at all times. (The operator should not have to pull out the Ballot Module to verify this, as we can be certain that some operators won't.)
- The IES 126 software should never be used for setting up or processing the results of an election without two people at the workstation agreeing about each step.

7.2 Recommendations

- IES Software used for counting an election should not have the maintenance code. It should not be compiled or loaded or linked into the counting version.

- Only those functions that are appropriate to a level should be executable at that level. Inappropriate functions shouldn't even appear in greyed-out form. If special overrides are required, they should be executed from a different program by a privileged user.
- Certification of all elections should be done at the service centres after the elections. These must corroborate the local election results. Where "mixing and numbering" and drawing lots are concerned, the local outcomes made should be available to the service level for confirmation.
- The machines must be cleared of any software that isn't to be used in the process. Unless there is a certified way of using these software elements to support the voting system safely, they should be removed; this includes drivers and software for such things as TCP/IP, Ethernet, and other things that could compromise security.

8 Using the Voting Machine from the Poll Worker's Perspective

The poll workers are responsible for arranging the Voting Machines in the voting hall, setting them up, testing them, running them during the election, removing the Ballot Modules at close-of-poll, sending the Ballot Modules to the service centre, and finally breaking down the Voting Machines and preparing them for shipment back to storage. Some of the poll workers will have a lot of training, some very little, and undoubtedly there will be some called in at the last moment who will get their training the morning of the election.

8.1 Setting up the machine

- Setting up this machine was complex, confusing and, at times, physically precarious. Carrying the voting machine is awkward. There is no balanced posture in which the machine could be carried with its handles.
- Opening the machine is confusing. The multiple latches and locks give apparent security. A tamper-proof seal is needed for actual security if a module is in the machine.
- Lifting the machine's voting panel into position is very awkward. It is heavy and unbalanced. To assemble it, the large lid must be raised vertically, while lifting the voting panel. A flimsy side shroud must be made to engage with the lid while holding the voting panel in the correct position. This takes strength and care. With average strength and balance, it was hard to figure out where to stand and how to hold everything to do it. In our experience the heavy and unbalanced design of the full-faced control surface is somewhat dangerous to manipulate. Even in the training video, with two people, the poll worker struggles to put the side panel in place to hold the control surface up.
- Placing the paper under the plastic was a challenge. The static charge on the plastic made it especially difficult. As soon as all five Ballot Papers were in place, sliding the plastic sheet over them dislodged them.
- The plastic cover is asymmetrical. If you flip it over, it will not fit onto the registration pegs.

- There is a line at the top of the Ballot Paper (in very tiny type) indicating which column of the Voting Machine the Ballot Paper belongs on. It will be difficult for many poll workers to read, and is subsequently hidden under the top aluminium bar.
- The Voting Machine stand allows three positions for voting from a wheelchair. We didn't have the special table shown in the video but it seemed from the video that the machine was in some danger of falling off the table.

8.2 Opening the Poll

- The process of holding down the function button while turning the key is error-prone.
- The console display does not give clear instructions to the operator.
- Administration (i.e., opening and closing the poll) uses the same key as running the poll.
- We did not see documentation for a way to test the backup module. It appears that anyone with a standard operating key can press the function key while turning the key, select "c" test voting machine mode, select clear backup, agree that they want to erase the backup and have cleared the backup memory from the machine.

8.3 Running the poll

- The operator uses the same key and the same control unit to run the election as is used to setup, open, and close it. This gives lots of room for both operator error and fraud.

8.4 Closing the poll

- Closing the poll and printing the end of poll statement took a long time. The Voting Machine has no progress bar or "expected time to run" indicator.

8.5 Critical Requirements

- The control unit (which controls the selection of the races available to each voter and determines the disposition of incomplete ballots [those that have not been confirmed by a second push on the cast vote button]) requires continuous oversight by at least one other person. It is crucial that someone besides the voter and the one operator can see the ballot activation and knows when the key is turned to eliminate an incomplete vote.
- In order to prevent erasure of the backup modules, when the poll is closed, the electricity supply to the voting machine must be discontinued and the module must be sealed.
- All backup modules must have serial numbers.

8.6 Recommendations

- The backup module in the machine should have a signed seal indicating that it has not been removed since being certified.

- The back-up battery should be capable of running the equipment for longer than the longest outage over the previous 10 years.
- A piece of tape applied to the top and bottom of the Ballot Paper would make it easy to place the Ballot Papers and not have them dislodge when replacing the plastic cover.
- Something should be done to make it obvious which column a Ballot Paper belongs in. Larger numbers on the Ballot Paper with matching numbers printed on the Voting Machine itself would help. Repositioning the registration pegs so that only the Ballot Paper with matching registration notches can fit would be better.
- Installing a gas-filled cylinder spring at each back corner of the machine would allow it to be opened safely.
- The voting machine stand should be fitted with a gas shock spring at each side to allow the machine to change positions easily. A linkage rod would allow a person in the front to pull a lever and rotate the machine without assistance. Mechanical stops would make it impossible to go beyond the limits of adjustment, thus preventing accidents.
- One physical key to set up and take down the machine and another for running it during voting would be more secure and simpler to use.
- The control unit display should indicate what buttons to use for what actions.
- The machine should beep in an identifiable way for the different settings as the poll worker manipulates the control box. This gives the poll worker feedback confirmation that they have set up the machine correctly. It also allows co-workers to notice what button was pushed.
- The potential for a poll worker using the machine in function mode to erase the backup module should be eliminated.

9 Using the Voting Machine from the Voter's Perspective

After verifying his/her registration by existing methods, the voter is given a colour-coded ticket, which is given in turn to the operator of the machine. The operator selects the set of races which the voter is eligible to vote in (European Parliament, County Council, Town Council, etc.) by pushing the appropriate colour-coded button on the control unit. The voter enters the polling booth, votes, and leaves. Some voters will have tried out the machines at exhibitions, some will have seen videos, most will have never seen the machine before, and some will have no experience with computers.

Entering the polling booth, the voter will see a series of ballot papers with candidates' names, party affiliations, and pictures (fig. 4). Next to the picture will be a pink "button" drawn on the paper (the actual button lies directly below) and next to that will be a bright, green LED display. The green LEDs will show double dashes ("- -") next to candidates whom the voter may vote for, and nothing for candidates in races which the voter cannot vote for. They will also show nothing next to blank spaces on the ballot.

The voter makes selections by pushing the pink buttons. When the voter selects the first candidate in a race, the green LEDs will display a bright “1.” A second selection will display a “2,” etc. Should the voter press the same button a second time, the preference for that candidate will be cleared (reset to dashes). Any other selections in that race with a higher number will also be cleared. (If the voter selects 1, 2, 3, and 4; then pushes 2 a second time; 2, 3, and 4 will all be cleared.) When the voter has made all desired selections, s/he completes the vote by pressing the “Cast Vote” button.

If not all of the races have been voted on and the voter presses the “Cast Vote” button, the machine gives a special beep and displays a blinking message on the yellow LED display at the top of the machine, telling the voter that the “Cast Vote” button must be pressed a second time if s/he does not want to vote in the remaining races. The voter may push “Cast Vote” a second time and record the vote as is, or may go back to the main panel and continue voting in the other races.

When all of the races have at least one selection, no second confirmation is required. If every candidate in every race has been voted for, the “Cast Vote” button will light up, indicating that there’s nothing else to do. Upon successful voting, the LED display clears before coming back with the confirmation that the ballot has been cast.

The issues we are concerned about include:

- Only the Voting Machine operator (looking at the control unit screen) and the voter in the booth can tell which set of races was activated. It is possible for the operator to partially disenfranchise voters by selecting the wrong set of races; many voters simply will not notice (see first-listed critical requirement under 8.5 above).
- The fact that no buttons on the voting machine give any physical “button feedback” is a concern.
- Some of our test-voters had difficulty with wanting to press the green displays, thinking they were the buttons. The mistake persisted even after the users understood that the button was the pink circle next to the candidate’s picture.
- The LED display at the top of the machine is not a focal point for the voter while making a selection. To read the name on the bottom of this display takes some effort.
- The Voting Machine does not allow a blank “protest ballot” to be cast.
- There is a keypad on the voting console (used when setting up and testing the machine). While it is in fact disabled during voting, it is still a distraction to the voter.
- The same key is used to express a preference and to cancel a preference.

9.1 Recommendations

- It would be valuable if the machine made a distinctive sound for each poll selected for a voter (Presidential Dáil European, Local, Referendum) giving feedback to the ballot worker that the correct set of polls had been enabled. All other ballot workers could also hear this

sound. The voter could use it as an indication that something had been done to their machine to set it up.

- When some races have not been voted on and the “Cast Vote” button is pressed, the display should stay lit and use its full height to display an animated arrow requesting confirmation accompanied by an audible beep. If a voter who has not voted in all races leaves the ballot booth having only pressed the cast vote once, the ballot should be deposited rather than cancelled.
- The machine should allow a protest ballot to be entered with no selections made. As with a ballot that has only some races selected, “Cast vote” should beep, display the fact that a blank ballot is about to be entered and require a second press.
- Some indication of how to operate the voting machine should be given. A poster on the back panel, facing the voter, is one possibility. It should be as simple as possible.
- If only two lines instead of three in the LED display were devoted to explanation and instructions the selected candidate name could be read more easily.
- The keypad in the voting machine should have a seal to prevent voters from attempting to tamper with it. In further development of the machine, the keypad might be moved to the control unit.
- We are considering the desirability of requiring two presses of the “Cast vote” button in all cases – one to submit the vote and the other to confirm it. This could be programmed in such a way that failure to press a second time would not jettison the vote. (This is a surprisingly problematic area. In other elections using electronic voting machines, votes are lost due to confusion over when to push the “Cast Vote” button. Indeed, the input-output test reported above provided evidence of possible problems in the use of the “Cast Vote” button).

Some of these comments may seem very minor, but they are important. The voters using these machines will see them once every few years for a few minutes. Some of the voters will have poor eyesight; many will feel intimidated by computers. Everything that distracts the voter will cause errors. Anything that *can* be done incorrectly, *will* be done incorrectly by someone.

10 Documentation

The Nedap/PowerVote Electronic voting and counting system documentation is used in conjunction with IES version 126 software. Overall, the tasks seem more complex than necessary. The procedures in the book attempt to break down the tasks into simple steps, but the complexity presented is still daunting.

The use of names for non-physical objects (computer data) is a tricky but important issue. Because the objects under discussion are “nebulous,” it is very easy for a computer user to become quite confused as to what s/he is working with and which object should do what. Thus the use of the word “poll” to mean: (a) The set of candidates for a specific position, (b) the set of all (a)s for a

specific election, (c) the location where people do their voting, and (d) perhaps several other slight shades of meaning, is a problem.

The authors could clarify the documentation by revisiting their terminology. The words “Election”, “Poll”, and “Ballot” have colloquial meanings and should be used with trepidation in naming data objects. People will get confused. Descriptive phrases such as “Ballot Paper” would facilitate understanding. For (a), “Race” might be reasonable, for (b) “Election” and for (c) “Polling Station”. “Level” is another term that is used ambiguously. Is “Service Level” the software being used, the set of functions in the software being used, a processing centre, a geographical location, or a specific building in that location?

- The manual discusses briefly how to set up County/City elections for “all the Local Electoral Areas ... together” or “...separately”, but gives little direction on the matter. The IES v126 appears not to support this (there is no “Local elections 2004” [the menu item shown in the manual] in the “New Poll” wizard).
- The manual states “A compatible file containing polling station data can be read into IES.” It says nothing more about this.
- The manual refers to the “PRU” without saying it is the Programming/Reading Unit.
- The term “Memory id” is used. It appears to mean “Ballot Module Identifier” but this isn't completely clear.
- On the last page of the operator’s guide, the following statement appears: “If you see a message in the display which consists of the following numbers, it means that the vote has not been stored. 8001, 8002, 5503, 5504.” These error messages should be clearer.
- Every data object which the IES user sees should be described clearly, along with a diagram of how they all fit together.
- Every operation the IES user executes should have a clear and unambiguous purpose. It should be obvious to the user what to do next and why.

11 Security Measures

- The memory module snapped open and exposed readily available, labelled parts with no security provisions. Putting it back together without noticeable damage was simple.
- The Programming/Reading Unit seals peeled back easily without damage. Inside, the system is composed of some standard EPROMs and a 68000 computer with standard 7400H TTL logic.
- The seals on the voting machine peeled back equally easily. Four Philips head screws had to be removed. The voting machine uses the same circuit board as the Programming/Reading Unit, only with different peripherals plugged into the numerous (11!) connectors.

11.1 Critical Requirements

- Effective protection against reprogramming ballot module memories before they are read must be put in place. This could be achieved by means of signed seals on the programming slot on the Programming/Reading Unit.
- All software in all portions of the system should be authenticated. It is worthwhile noting that very little of the voting process is secret – the contents and order of the ballot papers, and the details of the votes (once they are not identifiable with the individual voter) are all public knowledge. The only requirement is that they be accurate. The only secret is the specific vote cast by a specific voter. Hence authentication²⁴ of data is essential, but not encryption.

11.2 Recommendations

- A seal with a serial number on it that will be destroyed if peeled off, or a better lock must be associated with the programming slot of the memory module.
- Modules should have unforgeable serial numbers.
- Modules should be unopenable.

12 Conclusion

This report has reviewed previous evaluations of the Nedap/Powervote electronic voting system and has examined the process involved and its potential vulnerabilities. In the light of these considerations, we have conducted a range of tests of the hardware and software. These tests have included an input-output test of a representative sample of the deployed voting machines and tests of the system from the point of view of all the actors involved (officials, poll workers and voters). We have found no evidence of malfunction or malicious interference. We have, however, found evidence of a minor propensity to human error in inputting data into the machines. It is difficult to say whether real voters would be subject to such error and, if so, to what extent. The conjectural nature of our knowledge in this regard points to the need for further experimental study of the human-machine interface. It seems highly likely that the input of postal votes would be vulnerable to the input-error processes we have identified and steps would need to be taken to minimise this.

In evaluating and testing the system, we have identified a substantial number of critical requirements that must be implemented if future malfunction or interference is to be prevented. We have also identified a large number of recommendations, implementation of which would significantly improve the operation of the system. We would also like to emphasise that the combined results of our input-output test of the machines and of our tests of the usability of the machines point to the need for further experimental research on the human-machine interface.

²⁴Digital Authentication is a technique by which we can be certain that a given file (or any data) is exactly the file which the author wrote. If someone changes the contents of the file, we will know it. The basic idea is that the author uses a “secret key” (a big number) to create a “fancy checksum” (another number created by adding up all the bytes in the file and combining them with the key). The author then publishes a “public key” (another big number, related to the private key). Anyone may use the public key to verify that the checksum is correct, but they cannot create a new checksum. Mathematicians tell us that a 1024 bit key would take thousands of computer-years to crack.

Overall, however, we conclude (a) that the voting machines deployed for use in the June 2004 European and Local elections are a reliable means of recording the votes of the people and (b) that, provided that our critical requirements are implemented and that the aspects of the system we have not examined are shown to be satisfactory, the chosen electronic voting system can be safely used in the June 2004 elections.

The Research Team

Professor Richard Sinnott is Director of the Public Opinion and Political Behaviour research programme at the Institute for the Study of Social Change, University College Dublin. He is the author of *Irish Voters Decide* (Manchester University Press, 1995), and of numerous papers on Irish and European public opinion and political behaviour.

Professor Ted Selker is co-director of the Caltech/MIT voting project and runs the Context-Aware Computing group (www.media.mit.edu/context) at the MIT Media Laboratory. Prior to joining the MIT faculty in November 1999, he was an IBM fellow and adjunct professor at Stanford University. He has had product responsibility for many IBM products. He was a researcher at Xerox PARC. He is the author of numerous patents and papers.

Bil Lewis is a computer scientist who has worked on natural language understanding, expert systems, language design, and programming tools. He has taught at Stanford University and for numerous companies. He has worked at Stanford Research Institute, the FMC AI Center, and Sun Microsystems. His publications include *GNU Emacs Lisp*, the *Threads Primer*, *Multithreaded Programming with PThreads*, and *Multithreaded Programming with Java*.

Professor Brendan Whelan has been the Director of the ESRI since October 1996. He was previously a Research Professor and Head of the Survey Unit at the Institute. His research has been mainly concerned with the application of statistical methods to the collection and analysis of economic and social data, with particular reference to voting patterns, labour market issues, poverty and social exclusion.

Professor James Williams is Director of the ESRI's Survey Unit. He is currently a member of the group of experts working on the Joint Harmonised Business and Consumer Surveys for the European Commission. He is also a member of the International Advisory Committee for the Millennium Cohort Study in Britain. He has authored numerous research reports and publications on a wide array of topics and themes. His most recent publications have been on income distribution, poverty, survey techniques and labour market issues.

James McBride is Director of the Irish Social Science Data Archive, a joint UCD-ESRI initiative based at the Institute for the Study of Social Change, UCD. His research interests include electoral systems and public opinion.

