Testing, Accuracy and Secrecy

of the

Powervote / Nedap Electronic Voting System

A submission to the

Commission on Electronic Voting and Counting

by

J P McCarthy BSc FICS MIEI
Chartered Engineer
Management Consultant
Election Agent

Friday 26th March 2004

Table of Contents

Preface

Extracts may be freely quoted with attribution. I would appreciate a copy of any article quoting from this report. Please send them to joe.mccarthy at arkaon.com.

Joe McCarthy

01 607 7116
086 245 6788

1 Introduction

My ability to make a fully qualified submission to you is hampered by a lack of information. Despite 9 requests since October 2002 with 5 internal reviews and 5 appeals to the Information Commissioner I have been unable to obtain the documentation necessary to fully understand the electronic voting and counting systems. The Department has refused to release many relevant documents on the basis of Sections 27(1)(a) and 27(1)(b) of the FoI Act citing commercial sensitivity and trade secrets.

My findings and conclusions are based on the records released by the Department. I am happy to stand corrected in the light of further materials released.

I believe the Department is now swamped by the complexity of the project and in the words of Mr Tom Corcoran, the Assistant Secretary in charge of this project:

> "This is no ordinary project where it can often be sufficient to stagger over the line with perhaps not everything in place by completion date. We get only one opportunity at delivery and this has to be as near perfect as possible because of the fundamental and pre-eminent value of the democratic process and flowing from this, the extremely high level of media and public scrutiny."

This submission makes the following points:

- Essential aspects of the statutory rules have not been tested.
- The currency of the tests is now out of date.
- Certificates have not been issued for all tests.
- The testing agencies are not accredited in all cases.
- Issues raised by testers have not been addressed.

Accuracy

1. No formal methodology has been used to assess the accuracy of the system.
2. No criteria for accuracy of the system have been published.
3. Other than the counting software, the system has not been tested for accuracy.
4. The accurate operation of the system cannot be verified by the voter, by the Presiding Officer, by the Returning Officer or by the election agent.

Testing

5. The electronic voting system has not been fully tested.
6. The testing which has been carried out was inadequate.
7. Significant parts of the system have not been tested.
8. The counting software has only been partially tested in a "black-box" manner.
9. There is no tangible guarantee that components which will be used are the same as those which were tested.

Secrecy

10. The system infringes the secrecy of the ballot for voters who wish to abstain.
11. The embedded software in the voting machines is a proprietary trade secret.
12. The documentation describing the system is a commercially sensitive secret.

In summary, this system has not been specified accurately, has not been implemented constitutionally and has not been fully tested.

It is therefore an unsafe system and should not be used as it stands.

The only person who may constitutionally verify their vote is the voter. This can only be done using paper.

1.1 *Accuracy*

The following aspects of the Powervote / Nedap electronic voting system can be considered under this heading:

- Does the system accurately reflect the will of the people?
- Does the system faithfully record votes and count them accurately?
- Does the system accurately implement the Irish Statutory rules for elections?
- Has the system been tested end to end for accuracy?

1.2 *Testing*

The following aspects of the Powervote / Nedap electronic voting system can be considered under this heading:

- Have comprehensive tests been defined?
- Which tests have been run?
- Have these tests been passed?
- Have all tests have been independently verified?

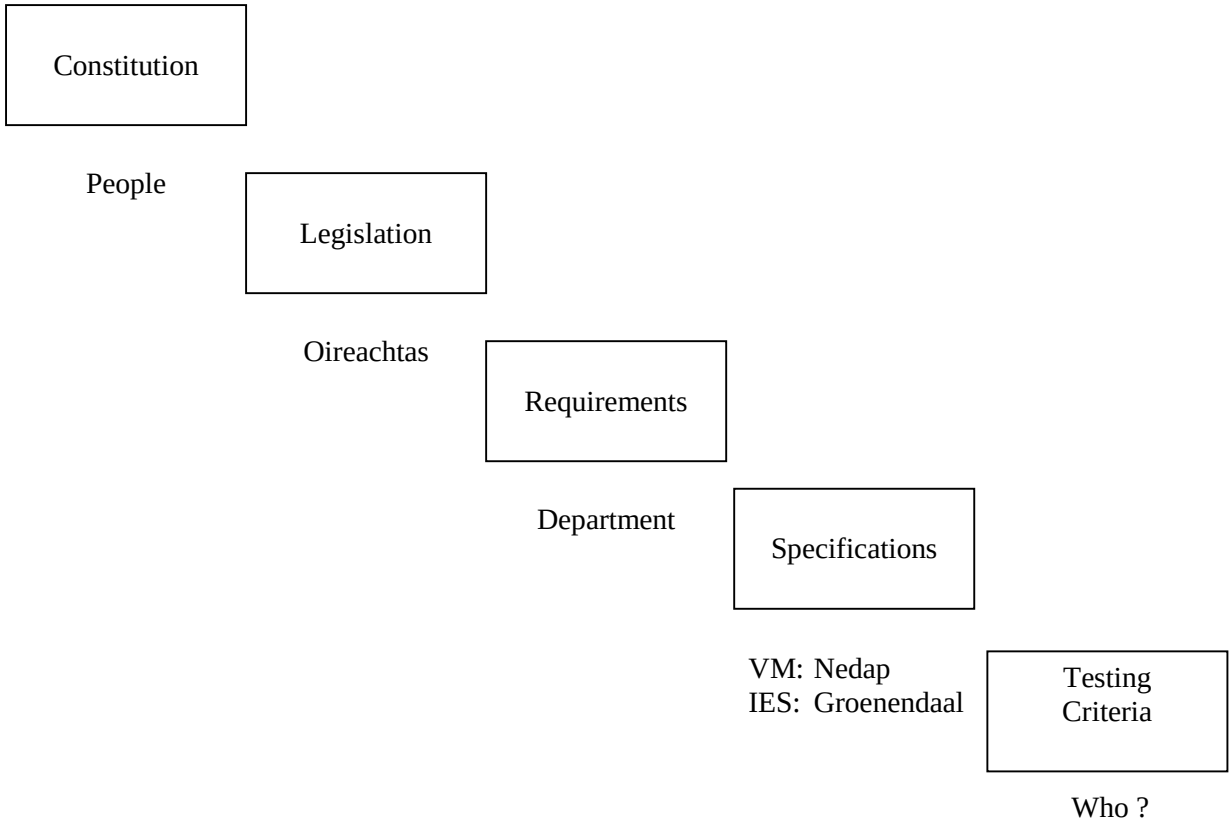
1.3 *Secrecy*

The following aspects of the Powervote / Nedap electronic voting system can be considered under this heading:

- Secrecy of the ballot
- Secrecy of the proprietary design of the hardware and software of the system
- Secrecy of the Department's handling of this project

2 Accuracy of Design

The proper design and accuracy of the electronic voting system must be assessed on the basis of defined requirements. In the case of our electoral system the basis for these requirements stems from our written constitution. A logical sequence should be followed as illustrated below. The owner of each step is shown with the notable absence of an owner for the test criteria.



O'Duffy , G (2000) *Count Requirements and Commentary on Count Rules*. Dublin: DoEHLG
O'Duffy , G (2001, 2002) *Count Requirements and Commentary on Count Rules.* Dublin: DoEHLG *Update No 1 to Update No 7*
Teunissen, RBW (2003) *Functional Specification -Nedap Voting System ESI2 – Powervote*, Holland: Nedap Specials
IT Unit (2003) *DVREC-2 – Requirements for Voting Machines for Use at Elections in Ireland.* Dublin: DoEHLG

2.1 *Constitution*

The Irish electronic voting system must meet a number of fixed external requirements derived from our written Constitution and from the statutory rules set out in legislation.

The public has ready access to the constitution and to the legislation.

Our rights as citizens derive from the Constitution where "*We, the people of Éire*"[1] have the "*right to designate the rulers of the State*"[2] using the "*secret ballot*" and "*on*

[1] *Constitution of Ireland*, preamble

the system of proportional representation by means of the single transferable vote"[3] in "*elections … regulated by law*"[4].

Note that both the Dutch and the German authorities have used their own national institutes to test and approve the voting machine to be used in their jurisdictions.

We should insist that the testing for Irish machines be done in Ireland.

A question arises as to the ability of the Irish Courts to review the system given that the developers and manufacturers are based in the Netherlands and are consequently outside the jurisdiction of the High Court.

2.2 *Legislation*

The Electoral Acts set out the procedures and rules for election in precise detail:

- Electoral Act 1992 (the Principal Act)
- Electoral (Amendment) Act 2001
- Electoral (Amendment) Act 2002
- Electoral (Amendment) (No 2) Act 2002

known together as the Electoral Acts, 1992 to 2002.

The Taoiseach announced in the Dáil that legislation to completely re-enact the Electoral Act will be introduced. This leaves the legal basis for the electronic voting system in an uncertain state at the time when this submission was made.

Part XIX of the Principal Act as amended sets out the counting rules. This part consisting of Sections 118 to 128 together with Sections 48(1) and Sections 114 to 116 was included in the Department's Request for Tender.

2.3 *Requirements*

The Department issued a Request for Tenders in June 2000 which included a separate document entitled: "Count Requirements and Commentary on Count Rules". This commentary document was written by Gabriel O'Duffy in the Department and it serves as a user requirements document for the counting software.

This document has been updated at least seven times with seven Update documents published by the Department. These updates address the following:

	Date	**Purpose**
Update 1	23 Feb 2001	Corrections, reports, **Petitions** with options left open to the programmer
Update 2	9 April 2001	Last Seat Shortcuts Candidates with zero votes

[2] ibid, Article 6
[3] Ibid, Articles 12.2.3°, 16.2.5° and 18.5
[4] Ibid, Articles 12.5 and 16.7

		Report Writing
Update 3	1 Oct 2001	Reconciliation of Voter Accounts Accounting for null votes
Update 4	2 Oct 2001	Changes to count rules due to High Court decision re deposits
Update 5	8 Jan 2002	Correct bugs in report screens
Update 6	14 Mar 2002	New requirement to export tables
Update 7	14 Apr 2002	Handling anomalies found by ERS testing where candidate(s) have zero votes

Further Updates	unpublished	Under debate between DoEHLG and Groenendaal

The requirements for reconciling, mixing and counting make no provision for invalid data in the system. Such invalid data may arise if mistakes are made by the programmers of the system or if external events occur which might alter the data. To proceed in a complex suite of software such as this without providing for such errors is foolhardy.

Indeed this approach is mandated in legislation by Section 45(3) of the 2001 Act:

> (3) Section 119(1) of the Principal Act, as so applied, shall have effect as if the reference in that section to section 114 were a reference to *section 44* of this Act and the words ", rejecting any that are invalid," were deleted.

The assumption inherent in this approach is that the computer is always 100% perfect. The

2.3.1 Complexity

The Count Requirements document is 172 pages long with over 35,000 words in some 2100 paragraphs. It is extremely complex. The Updates which have been issued are also complex. Further updates are being debated between the Department and the developers in a manner which gives cause for concern as to who is the real owner of the requirements. This debate is ongoing leaving us without a final set of requirements.

2.4 *Specifications*

Access to the specifications documentation has proved difficult to obtain.

Relevant documents are:

Published:

- Request For Tenders
- Functional Specification

Not published but obtained under FoI:

- Count Requirements and Commentary on Count Rules

- DVREC

Not published:
- Nedap documentation

2.4.1 Systems Documentation

Nedap material	Extensive but not all published
Groenendaal material	None !
Manuals for Returning Officers	Published

2.5 *Testing Criteria*

Formal testing criteria have not been set out in legislation, have not been set out in the requirements and have not been developed in the specifications.

The contract for the system does not require acceptance testing to be passed before payment for the machines is due to be paid.

2.5.1 Ministerial Approval

The criteria for approval of an electronic voting system are not set down in writing.

The relevant section of the 2001 Act is:

> **36.**—(1) Notwithstanding the provisions contained in Parts XVII, XVIII and XIX of the Principal Act, voting and vote counting at a Dáil election may be undertaken on voting system equipment approved for such purposes by the Minister.

Formal testing criteria have not been published.
Formal approval criteria have not been published.

Usually the testing criteria for a computer system are set out by the client. Detailed testing parameters are then developed by the authors of the system.

PTB derived some test requirements for the VM software from DVREC-2.

2.5.2 Acceptance Tests

The testing of the Powervote / Nedap system commissioned by the Department is a piecemeal affair.

- Three formal external tests.
- One black box external test
- One code and architectural review
- One general security review

Having been granted an opportunity to review the testing files in the Department it is clear to me that testing has proceeded on an ad-hoc basis.

Using FoI, I requested copies of test plans from the Department.

- There is no overall test plan.

- There is no regression test plan for new releases of software.

2.6 *Secure Coding & Testing*

There is no evidence that formal methods of testing have been used during the implementation of the electronic voting system for Ireland.

In the absence of a published test plan or formal approval criteria and with an incomplete set of actual test reports I have to refer to the literature to suggest what standards should have been applied.

References to testing techniques can be found in *Security Engineering* (Anderson, 2001)[5] where Ross Anderson gives guidance on system evaluation and assurance. In my professional opinion, this book is mandatory reading for anyone embarking on the development of a safety-critical system such as an electronic voting system.

I put the following questions to the Department and their response is quoted below:

2.6.1 Secure Coding Methods

Were any used in developing these systems?
Which ones?
Was Bruce Schneier consulted?
Was Ross Anderson consulted?
If not, why not?

Response

The credentials of Nedap and Powervote's system and staff are borne out by the results of continuous independent reviews which span more than 15 years. Neither Bruce Schneier nor Ross Anderson were consulted as it was not considered necessary, given the extensive independent testing that has been carried out on all aspects of the Nedap-Powervote system.

This response by the Department does not address the main question posed: What secure coding methods were used? They cite extensive independent tests of all aspects as an alternative. The independent testing was not extensive and did not test many aspects of the system – see below.

2.6.2 Evaluation & Assurance

The purpose of the testing of the electronic voting system is presumably to provide an evaluation or an assurance of the system. I say presumably because the Department have not published any criteria for their testing as such.

The difference between "*evaluation*" and "*assurance*" can be seen from the following quotations from Chapter 23 of *Security Engineering* by Anderson. Anderson is writing about computer security but the principles outlined by him apply equally well to the accuracy of voting systems.

23.2 Assurance

A working definition *of assurance* could be "our estimate of the likelihood that a system will not fail in some particular way." This estimate can be based on a number of factors, such

[5] Anderson, Ross (2001) *Security Engineering*, New York: Wiley.

as the process used to develop the system; the identity of the person or team who developed it; particular technical assessments, such as **the use of formal methods** or the deliberate introduction of a number of bugs to see how many of them are caught by the testing team; and experience—which ultimately depends on having **a model of how reliability grows** (or decays) over time as a system is subjected to testing, use, and maintenance.

23.2.2 Project Assurance

Assurance is a process very much like the development of code or documents. Just as you will have bugs in your code and in your specification, you will also have bugs in your test procedures. So assurance can be done as a one-off project or be the subject of continuous evolution. An example of the latter is given by the huge databases of known computer viruses that anti-virus software vendors accumulate over the years to do regression-testing of their products. Assurance can also involve a combination, as when a step in an evolutionary development is managed using project techniques and is tested as a feature before being integrated and subjected to system-level regression tests. Here, you also have to find ways of building feature tests into your **regression test suite**.

23.3 Evaluation

A working definition of ***evaluation* is "the process of assembling evidence** that a system meets, or fails to meet, a prescribed assurance target." (Evaluation often overlaps with testing, and is sometimes confused with it.) As I mentioned, this evidence might be needed only to convince your boss that you've completed the job. But, often, it is needed to reassure principals who will rely on the system that the principal who developed it, or who operates it, has done a workmanlike job. The fundamental problem is the tension that arises when the party who implements the protection and the party who relies on it are different.

Sometimes the tension is simple and visible, as when you design a burglar alarm to standards set by insurance underwriters, and have it certified by inspectors at the insurers' laboratories. Sometimes it's still visible but more complex, as when designing to government security standards that try to reconcile dozens of conflicting institutional interests, or when hiring your company's auditors to review a system and tell your boss that it's fit for purpose. It is harder when multiple principals are involved; for example, when a smartcard vendor wants an evaluation certificate from a government agency (which is trying to encourage the use of some feature such as key escrow that is in no one else's interest), in order to sell the card to a bank, which in turn wants to use it to dump the liability for fraud on to its customers. That may seem all rather crooked; but there may be no clearly criminal conduct by any of the people involved. The crookedness may be an emergent property that arises from managers following their own personal and departmental imperatives.

For example, managers often buy products and services that they know to be sub-optimal or even defective, but which are from big-name suppliers. This is known to minimize the likelihood of getting fired when things go wrong. Corporate lawyers don't condemn this as fraud, but praise it as due diligence. The end result may be that the relying party, the customer, has no say whatsoever, and will find it hard to get redress against the bank, the vendor, the evaluator, or the government when things go wrong.

Another serious and pervasive problem is that the words "assurance" and "evaluation" are often interpreted to apply only to the technical aspects of the system, and ignore usability (not to mention the even wider issues of appropriate internal controls and good corporate governance). Company directors also want assurance — that the directed procedures are followed, that there are no material errors in the accounts, that applicable laws are being complied with, and dozens of other things. But many evaluation schemes (especially the Common Criteria) studiously ignore the human and organizational elements in the system. If any thought is paid to them at all, the evaluation of these elements is considered to be a matter for the client's IT auditors, or even for a system administrator setting up configuration files. All that said, I'll focus on technical evaluation in what follows.

It is convenient to break evaluation into two cases. The first is where the evaluation is performed by **the relying party**; this includes insurance assessments, the independent verification and validation done by NASA on mission-critical code, and the previous generation of military evaluation criteria, such as the Orange Book. The second is where the evaluation is done by **someone other than the relying party**. Nowadays, this often means the Common Criteria evaluation process.

The approach to testing this system should be based on accepted principles for testing complex software systems.

The following extract from *Building Secure Software* (Viega & McGraw, 2002)[6] p.42 is directly relevant to the "Black Box" testing carried out by ERS:

> **Black Box Testing**
>
> Simply put, black box testing for security is not very effective. In fact, even without security in the picture, **black box testing is nowhere near as effective as white box testing** (making use of the architecture and code to understand how to write effective tests). **Testing is incredibly hard**. Just making sure every line of code is executed is often a nearly impossible task, never mind following every possible execution path, or even the far simpler goal of executing every branch in every possible truth state.
>
> **Security tests should always be driven by a risk analysis**. To function, a system is forced to make security tradeoffs. Security testing is a useful tool for probing the edges and boundaries of a tradeoff. Testing the risks can help determine how much risk is involved in the final implementation.
>
> Security testing should answer the question, "Is the system secure enough?" not the question, "Does this system have reliability problems?" The latter question can always be answered *Yes.*

And from page 39 of the same book:

> **Security Testing**
>
> Functional testing involves dynamically probing a system to determine whether the system does what it is supposed to do under normal circumstances. Security testing, when done well, is different. **Security testing involves probing a system in ways that an attacker might probe it, looking for weaknesses** in the software that can be exploited.
>
> Security testing is most effective when it is directed by system risks that are unearthed during **an architectural-level risk analysis**. This implies that security testing is a fundamentally creative form of testing that is only as strong as the risk analysis it is based on. Security testing is by its nature bounded by identified risks (as well as the security expertise of the tester).
>
> **Code coverage** has been shown to be a good metric for understanding how good a particular set of tests is at uncovering faults. It is always a good idea to use code coverage as a metric for measuring the effectiveness of functional testing. In terms of security testing, code coverage plays an even more critical role. Simply put, if there are areas of a program that have never been exercised during testing (either functional or security), these areas should be immediately suspect in terms of security. One obvious risk is that unexercised code will include Trojan horse functionality, whereby seemingly innocuous code carries out an attack. Less obvious (but more pervasive) is **the risk that unexercised code has serious bugs** that can be leveraged into a successful attack.

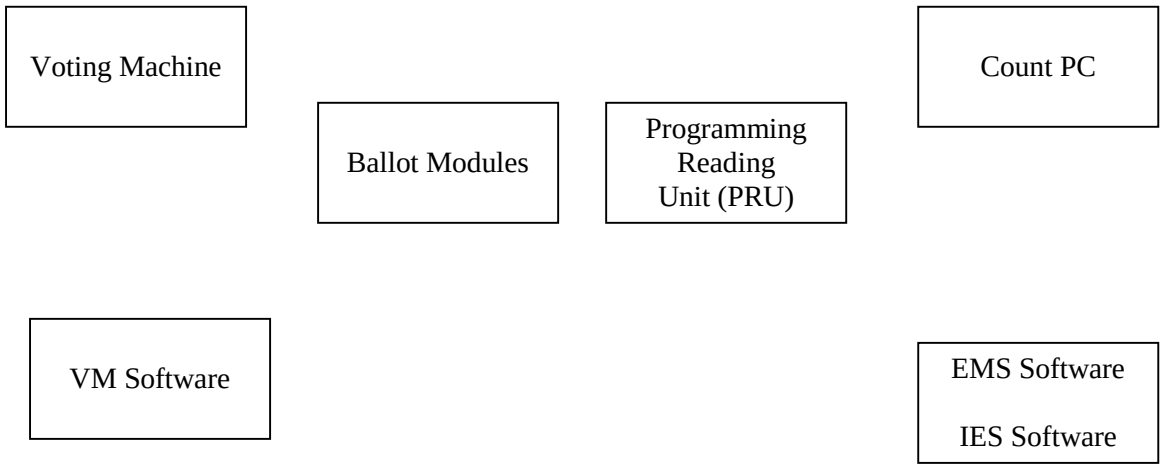
[The emphasis **in bold yellow** in the above quotations is mine,]

Note the authors' comment that "*Testing is incredibly hard*". There is no evidence that the Department has conducted a comprehensive testing program on this project.

[6] Viega, J & McGraw, G (2002) *Building Secure Software*, Boston: Addison Wesley

2.7 *Deliverables to be Tested*

All the various products supplied by Powervote / Nedap / Groenedaal illustrated in the following diagram require testing.



2.7.1 Hardware to be tested

Voting Machine ESI 1
Voting Machine ESI 2
PRU
Ballot Module
Count PC

2.7.2 Software to be tested

Voting Machine Software

- Casting
- Collecting

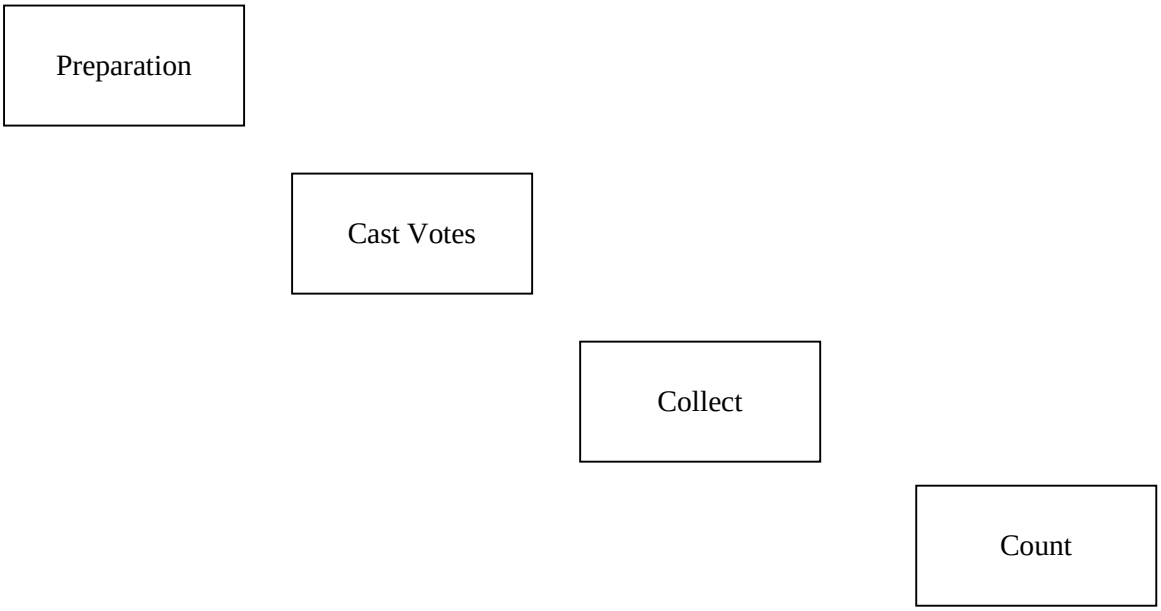
EMS – Election Administration software

- Polls
- Candidates
- Parties
- Electorate
- Polling stations
- Printed ballot layout
- Multiple ballot layout
- Loading ballot modules

IES – Integrated Election System

- Collecting
- Reconciling
- Mixing
- Counting
- Reporting

2.7.3 Election Activities to be Tested



Registration of electors
Constituency details
Warrant from Dáil to hold a poll
Order by Minister approving voting and counting machines
Guidelines issued by Minister

	Activity	Independent Testing						Accurate	Tested
		KEMA	TNO	PTB	ERS	Zerflow	Nathean		
	Preparation Returning Officer								
1.	Polls						R		
2.	Candidates						R		
3.	Parties						R		
4.	Electorate						R		
5.	Polling Stations						R		
6.	Printed Ballot Layout						R		
7.	Multiple ballot layout						R		
8.	Loading ballot modules			√					√
9.	ensure VM is working								
	Polling Station Pre-poll								
10.	Print candidates / no votes						R		
	Voter Authentication								
11.	PO identifies voter & issues token								
12.	Voter presents token								
	Cast vote								
13.	Official enables ballot(s)								
14.	Voter presses preferences								
15.	Voter presses "Cast Vote"								
16.	Deactivate VM if no vote cast								

	Activity	Independent Testing						Accurate	Tested
		KEMA	TNO	PTB	ERS	Zerflow	Nathean		
17.	Other voters use VM								
	Collect								
18.	Presiding Officer closes poll								
19.	Print out number of votes								
20.	Backup Ballot module loaded								
21.	Remove Ballot Module								
22.	Store VM with backup module								
23.	Transfer BM to Count Centre								
	Count Preparation								
24.	Postal ballots								
25.	Insert BM into PRU			√					
26.	Read in to PC						R		X
27.	Combine prefs into one ballot						R		X
28.	Write ballot to Access database						R		X
29.	Other BMs read in						R		X
30.	Reconcile votes						R		
31.	Mixing						R		
	Count								
32.	Counting						R		
33.	Quota						R		
34.	Each count						R		
35.	Distribute Surplus						R		
36.	Eliminate candidate						R		
37.	Evaluate LCC						R		
38.	Handle ties						R		
39.	Write sub-parcels to database						R		
40.	Declare result per count						R		
41.	Declare final result						R		
	Petitions								
42.	Petitions logic						?		

This matrix is incomplete. It serves as an aide-memoire to a Project Manager to help identify all the steps which have not been tested.

I was unable to complete the above matrix because I do not have a full set of records from the Department. It can be seen however that many aspects of the deliverables have not been tested by any independent agency.

The Department should be requested to elaborate this matrix, indicate the tests actually run and identify the remaining gaps.

It is clear that no complete test has yet taken place.

3 Review of Test Reports

The Minister and his Department commissioned reports from six companies. A statement issued by the Department on 2nd March says:

> "The integrity of the new electronic system has been vigorously tested by six independent, internationally accredited test institutes"[7]

The companies are listed below:

Company	Accredited	Test	Date	Comment
PTB	Yes	Voting Machine Type testing	17 Sept 2003	Irish Statutory requirements omitted
PTB		Voting Machine Software	17 Sept 2003	Irish Statutory requirements omitted
Kema	Yes	Mech & Elec tests	20 June 2003	
TNO	Yes	Mech & Elec tests	Jun – Oct 2003	
ERS	No	STV case tests	Dec 2003	"Black box"
Nathean	No	Code Review on Version 0111	23 Dec 2003	Desk check Out of date
		Architectural Review	23 Dec 2003	Desk check Out of date
Zerflow	Not known	Report	27 Mar 2002	Interim report
		Statement	4 July 2003	

Contrary to the Minister's statement only three of these companies are internationally accredited. See the Department's response under Topic 12 Certification in Questions to DoEHLG, Responses, Comments (McCarthy 2004)[8].

None of the test reports or certificates guarantees that the system implements the Irish statutory rules accurately.

3.1 *Stability of the software*

The Department and its reviewers do not yet have a stable version of the system. This constantly moving target makes it impossible for external reviewers such as myself to form an accurate opinion.

From the comments made by Nathean it is clear that they are suffering from the same difficulty in obtaining a stable set of code units for review.

[7] See Statement By Minister Martin Cullen TD On Electronic Voting 2nd March 2004 in Appendix.
[8] McCarthy, J (2004) *Questions to DoEHLG, Responses, Comments*, Dublin. Available from: http://evoting.cs.may.ie/Documents/QuestionswithDoEHLGResponses.doc [Accessed 25 March 2004]

I submit that the Commission will be confronted by the same issue of stability. When the question of a continuous stream of software releases was raised with the Department their response was:

> The Department will go on with this approach of continuous improvement between now and June 2004 and beyond that. We do not see this as any admission of weakness. The electronic voting system already meets high and satisfactory standards of performance. However, best practice means that we should not rest on our laurels and that we should add to margins of safety and reliability.

How can one improve a statutory set of count rules? Either the software meets the statutory requirements or it fails.

There is no log kept either by the Department or by the developer of bugs discovered during testing. There is a continuous stream of releases of versions of the IES software. When will it be stable?

After it has been stabilised how does the Department guarantee that the version of compiled software delivered is actually a true version of the source code as reviewed and tested?

There are no protocols or procedures in place to provide this guarantee of accuracy.

3.2 *PTB Reports*

PTB evaluated the design and software of the voting machine and the PRU. However, as quoted below, their testing excluded the Irish statutory requirements amongst other exclusions.

PTB state on page 3 of their report[9]:

> **1 General remarks**
>
> By letter of March 3, 2003 the PTB received the order to test the microprocessor-controlled voting machine ESI2_1 of the NEDAP N.V. company with the updated hardware version 3.00 and software version 2.00 in accordance with "*Functional specification - Nedap voting system ESI2 - Powervote*" and the new "*Requirements for voting machines for use at elections in Ireland DVREC-2", dated March 5, 2003*.
>
> The order for the test does not cover paragraphs 1.5, 4 (testing the voting machine against the Irish statutory requirements), 9.4, 11 (testing environmental conditions of the voting machine) and paragraph 12 (safety and health requirements for the manual handling of the voting machine), nor does it include the hardware tests of paragraphs 8.2, 8.3, 8.4, 10.2 and 10.3, which refer to paragraph 11 of the App. Part 1 to the "*Requirements for voting machines for use at elections in Ireland DVREC-2*".

When asked about the exclusion of the Irish statutory requirements, the Department replied[10]:

[9] Bronder, Th (2003) *Type testing of a voting machine for elections/referenda in Ireland*, Berlin: PTB
[10] Greene, P (2004), Debate on Electronic Voting, *Irish Times*, 20 February, Letters

> We agree with Mr McCarthy that the software testing undertaken by PTB (German National Institute for Science and Technology) did not include the statutory count rules. This was because testing of these rules was undertaken separately by the UK- based Electoral Reform Services.

My question did not refer to statutory count rules; rather it carefully referred to Irish statutory requirements. These requirements are set out in the Department's document *DVREC-2 Requirements for Voting Machines for use at Elections in Ireland*. The relevant sections which PTB were asked to ignore are quoted in full below:

> 1.5 The relevant statutory procedures for the preparation of a voting machine for a poll, use at a poll and at the close of a poll shall be capable of being performed by the voting machine. The word "poll" is deemed to include more than 1 poll (maximum 5) held simultaneously.
>
> 4. **Displaying ballot paper**
> The ballot paper displayed on the voting machine must comply with the Electoral Act, 1992, the Electoral (Amendment) Act, 2001 or relevant Ministerial Order under section 48 of the Act of 2001 and must be verified by statements printed from the voting machine before voting commences and at close of poll.
>
> 9.4 When the voter records a preference or casts a vote by means of the buttons on the voting machine, the following requirements shall apply to the buttons:
>
> - minimum dimensions: square 10 x 10 (mm), round 10 (mm);
> - maximum operating force for the selection of a candidate: 4(N);
> - maximum travel when buttons are pushed for selection of a preference for a candidate: 6(mm);
> - minimum travel when buttons are pushed: 0(mm).

PTB were not asked to test against the hardware tests of the following:

> 8.2 Subject to 10.3, a cast vote must not be lost by a power failure, the failing of one component, the effect of environmental conditions detailed in paragraph 11.1, through normal use or through failures in the operation of the voting machine.
>
> 8.3 The installed ballot module and its contents must be fully maintained in case of a power failure, the effect of environmental conditions as set out in paragraph 11.1, through normal use or through failures in the operation of the voting machine.
>
> 8.4 The functions of the voting machine must be fully maintained in the event of a power failure, or exposure to the environmental conditions as detailed in 11.1.
>
> 10.2 In the event of a power failure between 500 msec and 2000 msec of pressing the CAST VOTE(S) button, a vote stored in the Eeprom of the machine shall not be lost, providing there is no fatal machine failure on restoration of power.
>
> 10.3 In the event of a voting machine failure that affects the vote storage process (between 500 msec and 2000 msec of pressing the "CAST VOTE(S)" button), unless the failure is such as to cause a complete shut down of the machine, an error message shall be displayed e.g. error no. xxxx – vote not stored.

Note that the Department's reply stated "testing of these rules was undertaken separately by the UK- based Electoral Reform Services" Pindicating that ERS were to do these tests. But ERS have no role whatsoever in testing the voting machine. They have a very limited role in testing the counting functions of IES. Therefore nobody has tested the voting machines for the above requirements.

3.2.1 Change in Test Report Results

PTB first issued their test report on 30th June 2003 with several results listed as not OK. Their report was re-issued on 17th September 2003 with amendments to some of the comments and with seven results changed to OK.

Both reports referred to the one Nedap voting machine serial number R3D01028 and one PRU serial number NNE00010 with the one set of embedded software namely:

Typ:	Voting machine: Powervote - Integrated Election System ESI2,
Type:	Hardware version (Main) 03.00, (Connection) 01.00, (Display) 03.00 Software version (Main) 02.02, (Connection) 01.05, (Display) 02.01
Gerätenummer:	R3D01028 (ID-number of the prototype)
Serial number:	NNE00010 (ID-number of the Programming Unit)

The seven changed comments are tabulated here:

June version	
(39) **7.1** The voting machine shall **display**, where necessary, the total number of votes cast and, where applicable, the number of null votes; *At close of the poll the polling staff must turn the function switch key in the operating position while pressing the function button. The voting machine is now in the "Function" mode and the polling staff can close poll and show the votes cast on the display.* ***)** *The number of null votes can only be printed out, see note on (40)*	***NOK *)***
September version	
(39) **7.1** The voting machine shall **display**, where necessary, the total number of votes cast and, where applicable, the number of null votes; *At close of the poll the polling staff must turn the function switch key in the operating position while pressing the function button. The voting machine is now in the "Function" mode and the polling staff can close poll and show the votes cast on the display.* *The number of null votes can be printed out, see note on (40).*	***OK***
Difference	
None – but the result was changed from "NOK" to "OK".	

June version	
(45) **8.1** A vote recorded in the primary ballot module must be the vote that the voter has cast. *This requirement was checked by software tests (Encl. 1) only.*	***partly OK***
September version	
(45) **8.1** A vote recorded in the primary ballot module must be the vote that the voter has cast. *This requirement was checked by software tests (Encl. 1) only.*	***OK***
Difference	
None – but the result was changed from partly OK to OK.	

June version	
(49) 8.4 The functions of the voting machine must be fully maintained in the event of a power failure, or exposure to the environmental conditions as detailed in **11.1**. *a) This requirement was checked by software tests (Encl. 1) only.* *b) For tests regarding **environmental conditions,** see notes on paragraph **11.1.***	***largely OK***
September version	
(49) **8.4** The functions of the voting machine must be fully maintained in the event of a power failure, or exposure to the environmental conditions as detailed in **11.1**. *The printer and the fluorescent lamp do not work if a battery is used (see list 1 No. 1 "functional specification" in the Appendix of this Test Report).* *a) This requirement was checked by software tests (Encl. 1) only.* *b) For tests regarding **environmental conditions,** see notes on paragraph **11.1.***	***OK***
Difference	
Added sentence re printer and lamp – but the result was changed from largely OK to OK.	

June version	
(60) **8.7** The voting machine shall have a physical seal on the cover of the electronics unit to prevent the exchange or interference with program chips. ****) The requirement of this paragraph can not be tested at the prototype of the voting machine, it should be tested at serial machines.***	****)***
September version	
(60) **8.7** The voting machine shall have a physical seal on the cover of the electronics unit to prevent the exchange or interference with program chips. **) Provisions have been made at the prototype of the machine for a seal to be put on the electronic panel. A local inspection on serial machines is required.*	***OK *)***
Difference	
Different wording – result changed from "not tested" to "OK *)"	

June version	
(69) **10.3** In the event of a voting machine failure that affects the vote storage process (between 500 msec and 2000 msec of pressing the "CAST VOTE(S)" button), unless the failure is such as to cause a complete shut down of the machine, an error message shall be displayed e.g. error no. xxxx- vote not stored. *This requirement was checked by software tests (Encl. 1) only.*	***largely OK***
September version	
(69) **10.3** In the event of a voting machine failure that affects the vote storage process (between 500 msec and 2000 msec of pressing the "CAST VOTE(S)" button), unless the failure is such as to cause a complete shut down of the machine, an error message shall be displayed e.g. error no. xxxx- vote not stored. *This requirement was checked by software tests (Encl. 1) only.* **) While an error code is displayed, the message is not displayed, see note (72).*	***OK *)***

Difference
Sentence added. Result changed from “largely OK” to “OK *)”

June version	
(72) **10.6** The meaning of the fault messages generated by the diagnostic mechanism and the actions to be taken with respect to each fault message must be clearly stated in the voting machine user manual for help desk staff. *The meanings of the fault messages are not listed in the user manual.* *See list (3) No. 3 in Appendix of this Test Report.*	***NOK***
September version	
(72) **10.6** The meaning of the **fault messages** generated by the diagnostic mechanism and the actions to be taken with respect to each fault message must be clearly stated in the voting machine user manual for **help desk staff**. *The meanings of all error codes are listed in a special document in addition to the user manual. See note on (100) and list (3) “Documentation” No. 4 in the Appendix of this Test Report.*	***OK***
Difference	
Sentence added. Result was changed from “NOK” to “OK”.	

June version	
The **user manual** must include: *(100)* - manual handling requirements (Council Directive 90/269/EEC of 29 May 1990); *These handling requirements are not listed in the (draft of) the user manual.*	***NOK***
September version	
The **user manual** must include: *(100)* - manual handling requirements (Council Directive 90/269/EEC of 29 May 1990) (including a list of error codes and explanations); *In a special section “Troubleshooting” of the user manual **for the polling staff** there are listed 21 error codes (with instructions for the polling staff) which appear when the vote has not been stored.* *In addition to the user manual there is a document with a **full list of error/event codes** (and messages) **for help desc staff.*** *See list 3 "Documentation" No. 4 in the Appendix of this Test Report.*	***OK***
Difference	
Different comment. Result was changed from “NOK” to “OK”.	

3.2.2 Conclusion

An independent test report should be just that. Independent. Why did the Department see fit to review their report with PTB and seek changes to the result column to restate the results?

3.3 *Nathean Reports*

Nathean have conducted IES code reviews on behalf of the Department. It can be argued that code reviews do not constitute testing since no activity other than desk checking takes place in a code review.

Because the Nathean reports are the only independent source of information on the internal structures of the IES software, I believe that the Commission must take their reports into consideration under the Accuracy term of reference.

3.3.1 Nathean Code Review

The code review published by Nathean deals with version 0111 of IES whereas the ERS tests were conducted with version 0121. Neither version is the one to be used in June 2004.

The following sections are taken from the Nathean Code Review[11]:

> **1.0 INTRODUCTION**
> This document contains the code review sheets as updated during this evaluation of the source code units supplied relating to build 0111 (2003). These units relate specifically to the modifications made for the multielection processing. By agreement, Powervote did not supply any units which were not modified or specifically written for the Irish edition of the IES.
>
> **2.1 Outstanding Units**
> While all units have been supplied as requested, some units containing modifications as a result of this or previous reviews were supplied subsequent to the current review. These units are noted in the summary and detailed issue lists and should be evaluated in the next review.
>
> **3.0 SUMMARY OF ISSUES**
>
> No new significant issues have been raised during this examination. There were a number of new units in the review (approx 50). The vast majority of these new units relate to user interface forms, to updating election setup, and to the multi-election processing extensions.
>
> There were few changes to units relating to the processing of the count rules. In January 2004 we will request an up-to-date list of election rule modifications from Gabriel O'Byrne for cross-reference purposes.
>
> The current review gives the coding standards a clean bill of health. All previous recommended coding standards have been observed.

3.3.2 Comments on 1.0 Introduction

By agreement Nathean did NOT review any units other then the specific Irish units. This means that they have not reviewed some two thirds of the IES code. Nathean have stated that the code base is some 220,000 lines of code and Mr Hank Steentjes of Nedap told the Joint Committee on December 18th that 70,000 lines of code applied to Ireland.

Therefore, there has been no complete review by anyone of the IES software. The Irish people are therefore being asked to trust an untested system.

[11] Pugh, J (2003), *Code Review of IES Build 0111*, Dublin: Nathean Technologies

3.3.3 Comments on 2.0 Outstanding Units

Nathean state:

> While all units have been supplied as requested, **some units** containing modifications as a result of this or previous reviews **were supplied subsequent to the current review**.

The full suite of software was not available for Nathean to conduct their review.

3.3.4 Comments on 3.0 Summary of Issues

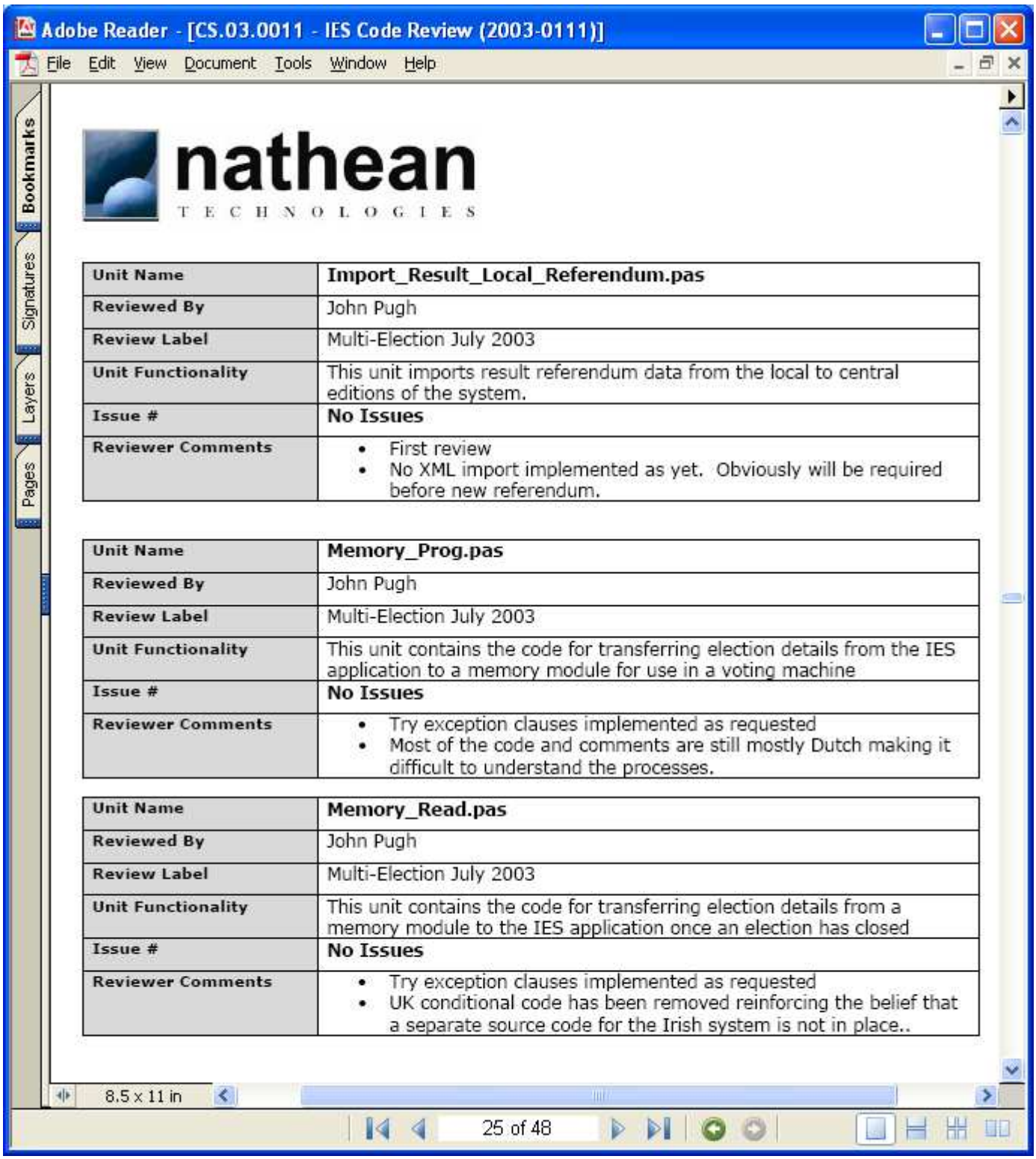
Nathean state that "an up-to-date list of election rule modifications from Gabriel O'Byrne" is still outstanding. [I believe this reference should be to Gabriel O'Duffy.]

This is a most extraordinary statement.

Without a definite specification of the election rules how could any reviewer certify that the software meets requirements?

3.3.5 Code Unit Issues

Some individual comments made by Nathean give rise to concern. Four are selected here:



Adobe Reader - [CS.03.0011 - IES Code Review (2003-0111)]

File Edit View Document Tools Window Help

Bookmarks Signatures Layers Pages

nathean TECHNOLOGIES

Unit Name	**Import_Result_Local_Referendum.pas**
Reviewed By	John Pugh
Review Label	Multi-Election July 2003
Unit Functionality	This unit imports result referendum data from the local to central editions of the system.
Issue #	**No Issues**
Reviewer Comments	• First review • No XML import implemented as yet. Obviously will be required before new referendum.

Unit Name	**Memory_Prog.pas**
Reviewed By	John Pugh
Review Label	Multi-Election July 2003
Unit Functionality	This unit contains the code for transferring election details from the IES application to a memory module for use in a voting machine
Issue #	**No Issues**
Reviewer Comments	• Try exception clauses implemented as requested • Most of the code and comments are still mostly Dutch making it difficult to understand the processes.

Unit Name	**Memory_Read.pas**
Reviewed By	John Pugh
Review Label	Multi-Election July 2003
Unit Functionality	This unit contains the code for transferring election details from a memory module to the IES application once an election has closed
Issue #	**No Issues**
Reviewer Comments	• Try exception clauses implemented as requested • UK conditional code has been removed reinforcing the belief that a separate source code for the Irish system is not in place..

8.5 x 11 in

25 of 48

The above extract from page 25 of the Nathean Code Review illustrates three important issues:

1. The software is not ready for a referendum
2. Some software is still written in Dutch
3. A separate code base for the Irish system is not in place.

The code units

The code units referred to above are Memory_Prog and Memory_Read. These are the very modules which read and write from the IES PC to the blue ballot modules.

It is at this point in the transfer of information and votes that errors are most likely to happen. The utmost care is required here to ensure the accuracy of the system. Yet, the code is written in Dutch. The transmission protocol used between the PRU and the PC is an old style start-stop serial protocol using STX, ETX and simple LRC mechanisms to transfer the data. These old protocols have no provision for error correction and force the application programmer to implement precautions to safeguard the integrity of the data.

There is no evidence that this has been implemented safely by Groenendaal.

On page 45 the reviewer comment shown below illustrates one of the absent code units which Nathean were unable to review. Note the reference to a function in a further code unit: Jansen.pas.

This is an important function for the accuracy of the system. Code unit Jensen.pas has not been reviewed.

Unit Name	**Secure_Database_1**
Reviewed By	John Pugh
Review Label	Multi-Election July 2003
Unit Functionality	First Review. This unit contains a single function Secure_Database which creates a copy of the election database.
Issue #	**No Issues**
Reviewer Comments •	• The function calls the JJCopyFile function which seems to be in the unit Jansen.pas. This will need to be evaluated.

3.3.6 Nathean Architectural Review

The following section is taken from the Nathean Architectural Review[12]:

> **Summary Findings**
> Powervote are investigating the above recommendations and are currently testing their impact on the IES application (e.g. with regard to speed). Powervote recommend deferring any modifications to the database until after the next election, given the proximity of the election and the validation process that is required by any such changes. Given that these modifications have not been required by any of Powervote's other clients, this sentiment is valid.

The recommendations referred to in this paragraph are

a) Convert the database from Access 97 to Access 2002.
b) Utilise Workgroup Information files (.mdw) in addition to a database password.
c) Implement database encryption to increase the inherent security of the IES database.

These recommendations go to the heart of the accuracy of the database used by Powervote.

[12] Pugh, J (2003) *Architectural Assessment of IES for use at June 2004 Elections (Build 0111)*, Dublin: Nathean Technologies

It should be noted that support by Microsoft for Access 97 has been withdrawn since 2001. The IES system therefore is relying on unsupported and out-of-date software.

Powervote do not have any other client for an STV system therefore Nathean's conclusion that "this sentiment is valid" has no sound basis. Powervote are using the proximity of an election and the burden of validation to avoid making obvious required changes. This is no way to develop robust systems.

The correct approach is to postpone use of the system until testing has proved it safe to use.

3.3.7 Conclusion

Nathean have reviewed an out-of-date version of the IES software.
Nathean only reviewed one third of the IES code base.
Nathean do not have the full set of counting requirements.
The review undertaken by Nathean of the Irish units is incomplete.
Relevant code units have never been reviewed.

3.4 *ERS Report*

The following is taken from the ERS report[13]:

> The test method adopted to ensure the IES software conforms to the STV rules required was the same as in 2002, *comparison testing*.
>
> **Comments**
> IES v93 had passed all tests in 2002 (in General election mode only, and using a slightly smaller database) and IES v121 has passed all tests again (with a larger database, under all three modes of Irish STV rules, and with enhanced testing of tie logic). However, errors were found in IES v112 to v119 (see Appendix B for details), and although these errors do not call into question the results declared for the 2002 general election pilots (the data from those pilots now forms three new test cases in the database and these test cases have passed the comparison testing with all versions of eSTV and IES on which they have been run), **we did begin to question whether our database of test cases, which we had believed was comprehensive enough to reveal any software errors, actually had an adequate number and variety of test cases for the purpose of testing IES and Irish STV rules.** [My emphasis]
>
> The parameters of an STV election – seats, candidates and votes – and the type of events which can take place – exclusions, surpluses, drawing of lots and so on – give rise to an unlimited universe of logically possible combinations.
>
> Even 425 test cases, though, allows a very wide range of possibilities for each parameter as the following tables show:
>
> **Table 2a: Parameter ranges**

Item	Minimum	Maximum
Number of seats	1	29
Number of candidates	3	49
Number of votes	4	999964
File size	88 bytes	12.5MB

[13] Wadsworth, J & Wichmann,B (2003) *Report on Irish STV Software Testing*, London: ERS

Table 2b: Case diversity

Case type	Number
Local result differs from General result	57
Bye result differs from General result	8
General results requiring drawing of lots for order of exclusion	119
General results requiring drawing of lots for order of surplus	23
General results requiring drawing of lots for allocation of surplus remainders	11

An alternative approach to comparison testing is to analyse the algorithms in great depth and produce test cases to cover each logically distinct case. However, we could not be certain that the implementation followed the same logical analysis – a different analysis would require different test cases. Also **analysis of the algorithms to the required depth is not easy**.[my emphasis] An implementation might deal with each type of event properly on its own, but fail when presented with those same events in a particular sequence (say, a tie for exclusion between three candidates, followed by a tie for allocation of surplus remainder between the two remaining lowest candidates, followed by their multiple exclusion). The combination and sequence of events may or may not have an effect, depending on the implementation logic, so it is difficult to know whether a test case is relevant.

The following comment made on Version 119 just a fortnight before their final approval of IES shows how dangerous it is to rely on black box testing:

V119	22/10/2003	52	S012C1 & many others. Apparently an unintended side-effect of previous fixes, this version of IES cuts the election short, declaring the highest continuing candidate elected even though several more stages are needed.
V121	03/11/2003	1275+9	All tests passed.

The unintended side-effect of earlier fixes is the sort of nightmare which besets all software developers. I asked the Department for a copy of their process for regression testing. They have no such process.

3.4.1 Conclusion

The only criterion used by ERS for their testing was a comparison with the results of their own eSTV results. Since they only did "comparison testing" it can not be said that they tested the Irish Statutory Count rules fully.

They identify the need to test the algorithms.
They identify the need for individual test cases.
They admit themselves that this would "not be easy".

Nobody said it had to be easy. Our constitution and our legislation mandate that it must be accurate.

They question whether their database of test cases is comprehensive. I submit that it cannot be comprehensive since they had no part in developing the software and they have no access to the source code.

3.5 *KEMA & TNO Reports*

The tests carried out by KEMA and TNO relate to hardware, electrical and environmental standards. These tests are not relevant to the Accuracy and Secrecy terms of reference of the Commission.

They do fall to be considered under the Testing term of reference.

The approval certificates supplied by TNO are dated in September 2003 which is after the manufacture and delivery of the Irish machines had begun.

3.6 *Zerflow Report*

This report was written in March 2002 by Colin English of Zerflow.

Chapter 4 Interim Report lists a number of issues of concern. These are quoted below:

> **4 Interim Report**
>
> Zerflow highlighted the following issues at a meeting with Peter Green. These issues arose from a discussion between Zerflow staff with little knowledge of the voting machine. It was after this meeting that Zerflow were requested to conduct a full review of the voting machine.
>
> **4.1 Immediate issues of concern**
>
> Issue 1. What actions and processes are audited, how is the audit trail linked, and who has access to that audit?
>
> Issue 2. In the case of dispute, is there any sort of recount, or manual input via audit trail?
>
> Issue 3. What facility is provided so that a voter can only vote in the allowed votes (e.g. A U.S. national cannot vote in Dail election, but can vote in local election)? If two polls held on same day, what stops this person voting in the Dail election?
>
> Issue 4. How does the system confirm that each vote has been accepted (or rejected) and recorded?
>
> Issue 5. If the system fails, what is in place to cope (e.g. electricity failure/ power surge)? If the system is inoperable, what system takes place?
>
> Issue 6. If the system fails during the days polling, and an alternative system is used, how are the two systems reconciled, and tabulated?
>
> Issue 7. How does the local poll centre staff know, and verify that the system is working correctly?
>
> Issue 8. If the system does fail, and an alternative system used, how is a guarantee given that the system is no longer operable by unauthorised persons?
>
> Issue 9. What is the fault tolerance, and how has it been validated?
>
> Issue 10. In the case of a dispute (e.g. at the count centre it transpires that a candidate expected to poll approx 7,000 first preference votes only gets 300, and a candidate normally expected to get approx. 300 votes, gets 7,000 votes. There has clearly been an error, and the candidates' details and recorded votes have been mixed up): does that election stand, is there a method of checking, can the audit trail provide any further information?

None of these issues were developed by Zerflow and none were subsequently addressed by the Department. A further list of findings was identified in Chapter 6 Technical Summary as shown below:

Finding 1. The front cover of the voting machine can be easily tampered with.

Finding 2. The key used to operate the control console is not secure

Finding 3. In the event of power loss, unless the control unit operator is keeping a constant count of votes there will be no way of knowing if a voter has actually cast a vote.

Finding 4. The rear cover for the voting machine should be made of metal and alarmed to prevent access to the cartridges.

Finding 5. Backup cartridges remain in the voting machine.

Finding 6. Backup cartridges can be wiped in the voting machine.

Finding 7. The voting machine should be powered off when accessing the cartridge or changing the paper.

Finding 8. Storage of cartridges after counting

Finding 9. The voting machine needs to be secured to a table by some means.

Finding 10. The voting machine does not display a CE compliance sticker

Finding 11. The data stored on the cartridges is not encrypted

Finding 12. The voting machine can only support a maximum of 56 candidates for a single election.

Finding 13. There may be an issue with voting machine availability during peak hours

Finding 14. The pictures of candidates and party symbols on the ballot paper are small and of bad quality

Finding 15. The Cast Vote button has no label indicating its purpose.

Finding 16. More handles are required on the voting machine.

Finally, in Chapter 7 Conclusions, Zerflow recommended:

- Formal policies and procedures to cover all eventualities regarding the voting machines and their use
- A third party audit be put in place to test the system on polling day in the next election, and to measure its performance
- A post election audit following the initial trial in the three constituencies in May 2002.

The recent statement by Minister Cullen says:

> "Zerflow Information Security Ltd undertook a rigorous security assessment of the system and confirmed that the measures introduced following the initial pilot elections have addressed any concerns they have with the system."

However the actual statement by Zerflow (copy attached) only addressed the first 6 findings listed above.

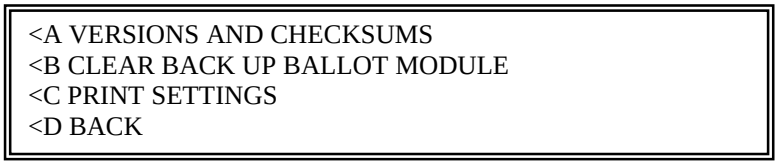
3.6.1 Finding 6

Zerflow's concern that the contents of the backup module can be wiped has not been addressed properly. The response from the Department was "*Only the returning officer or person authorised by him/her is permitted to wipe the backup cartridge.*" The problem will arise because of mistake or malice so the question of being "authorised" to do so is irrelevant. The following extract from page 5 of the Voting Machine[14] manual shows how easily this incident could come about:

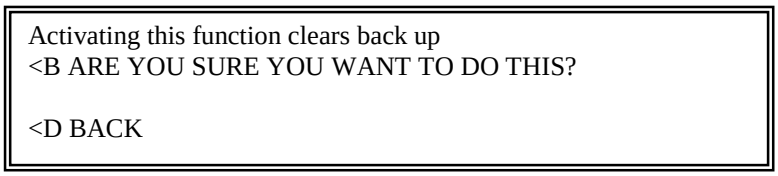
[14] Powervote (2003) *The Voting Machine 0906-1*, Dublin: Powervote Nedap

At the main menu.

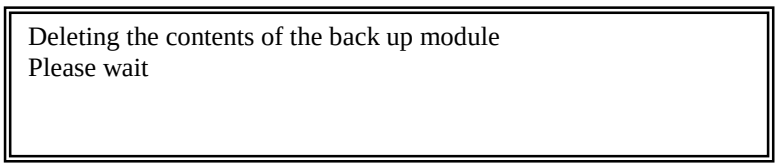
Press <D.



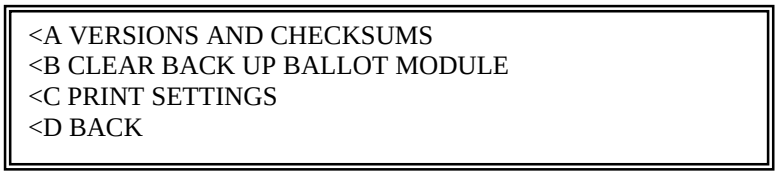
Press <B.



This is a precautionary measure to ensure that the module is cleared.
Press <B



During the process you will hear 4 beeps.



When completed the VD automatically returns to this screen.

Select <D to return to main menu.

It can be seen that it takes only two presses of button B to delete all votes from the backup module.

3.6.2 Finding 3

Zerflow's third finding was:

> In the event of power loss, unless the control unit operator is keeping a constant count of votes there will be no way of knowing if a voter has actually cast a vote.

The response from the Department was "*In the event of power loss, if a voter is in any doubt that their vote has not been cast successfully, a tally of the permit tickets and the number of votes cast on voting machines will provide a simple means of validating the vote count. The risk of this event occurring is minimal.*"

I wish to analyse the Departments response in detail.

- *In the event of power loss, if a voter is in any doubt that their vote has not been cast successfully,*

It is not up to the voter to ascertain if his vote has been cast successfully. It is the responsibility of the Minister, his Department and their suppliers to ensure this.

- *a tally of the permit tickets and the number of votes cast on voting machines*

This phrase refers to "machines" plural. Why is this? The voter after all has only been using one machine.

- *will provide a simple means of validating the vote count.*

The implication of this phrase is that there is a direct correlation between permits to vote and votes recorded. For three reasons this is likely to be untrue:

1. The voting machine does not always record votes just after a power failure depending on the timing between pressing the Cast Vote button and the actual power failure.

2. The list of errors published in the Voting Machine Operators Manual is shown below. It lists 15 different message codes which might arise each of which "*means that the vote is stored but NOT counted*".

3. A voter may walk away from the machine without voting thus no vote will be counted for his permit ticket.

Troubleshooting.

In the unlikely event that the voting machine does not function according to the procedure described call the help desk number provided.

The display above the voters panel will, in most circumstances show a message if a problem occurs.

Make a note of this message so that you can tell the help desk. This will help diagnosis of the problem and what action to take.

If you see a message in the display which consists of one of the following numbers it means that the vote has not been stored.

8001
8002
5406
5410
5503
5504

If you see a message in the display which consists of one of the following numbers it means that the vote is stored but NOT counted.

5104
5108
5112
5116
5118
5120
5122
5124
5126
5128
5129
5131
5132
5133
5139

The voting machine should be exchanged and the voter must be asked to choose their preferences again on this new voting machine and press the cast vote button.

The last instruction in the above extract from the Operators Manual means that the voter will be allowed to vote twice. This is extraordinary.

It is clear that Zerflow raised many important issues which have never been tested.

The Department was on notice from March 2002 that their external reviewers had identified the need for an audit trail. This issue was clearly identified by Zerflow yet the Department never pursued it.

3.7 *End to End Tests*

No end-to-end tests were conducted independently.

In the absence of an overall test plan, with definite pass / fail criteria, with a single co-ordinator to ensure it is carried out and with independent review of the test results we cannot trust this electronic voting system.

3.7.1 Pilot Trials

The trial conducted in Dublin and Meath in 2002 are irrelevant to the testing and accuracy of the current system.

Voting Machine ESI1 was used in 2002 for the June and November trials.

3.7.2 Foreign experience

Experience elsewhere with other versions of the Nedap machines gives no reassurance to the Irish public that the ESI2 machine can handle the Irish PR-STV system properly.

The machines used in Holland and Germany are quite different to the machines proposed for Ireland.

The voting system is different – single vote not transferable

- Different hardware
- Different software
- Different counting rules – much simpler
- Only one button per ballot in Netherlands
- One button on each of two ballots in Germany
- Results printed out on the machine itself at the end of polling

Therefore reference to satisfactory usage by 70,000,000 voters is irrelevant to the Irish situation.

We have a new machine with new software for a new voting system never before used outside Ireland.

The ESI2 machine is unique to Ireland. It has never been used elsewhere. It has never been piloted in Ireland.

ESI2 is different machine:

- Different buttons
- LEDs instead of LCDs
- Different software

4 Statement by Minister

Statement By Minister Martin Cullen TD On Electronic Voting, 2nd March 2004:

The integrity of the new electronic system has been vigorously tested by six independent, internationally accredited test institutes:

- Physikalisch-Technische Bundesanstalt (PTB), the German institute which tested the voting machine software, confirming that it performs all the tasks required and that it has sufficient internal checks to identify any attempted interference.
- Nathean Technologies, an Irish software firm, undertook an architectural code review of the election software and concluded that the code does not contain elements which can corrupt the correct running of the software.
- The Electoral Reform Society in the UK tested the PR STV (Single Transferable Vote) count rules against the 400+ STV elections in their database to ensure that the rules have been precisely applied.
- Zerflow Information Security Ltd undertook a rigorous security assessment of the system and confirmed that the measures introduced following the initial pilot elections have addressed any concerns they have with the system.
- Kema Quality BV (accredited by Dutch Council for accreditation) examined and certified the physical voting machine components.
- TNO, the Dutch Electronic Products and Services company tested the voting machine and supporting equipment for compliance with international standards for environmental conditions (such as temperature, humidity, power supply voltage and interruptions, electromagnetic compatibility, insulation, energy consumption and transportation).

5 Appendix A - CEV Invitation

"The Commission on Electronic Voting invites the public to make submissions to it in relation to its work, specifically, on the secrecy and accuracy of the chosen Nedap/Powervote electronic voting system and the testing thereof."

5.1 *Terms of Reference*

1. The Commission, which shall be independent in the performance of its functions, shall prepare a number of reports for presentation to the Ceann Comhairle (the Chairman of Dáil Éireann) on the secrecy and accuracy of the chosen electronic voting and counting system i.e. the Powervote/Nedap system.

2. The Commission shall make one or more of such reports to the Ceann Comhairle not later than 1 May, 2004.

3. The Commission's subsequent report or reports will record its views of the operation and experience of electronic voting and counting at elections.

4. In carrying out its work, it will be open to the Commission to review the tests already undertaken to validate the electronic voting and counting system and to have further tests undertaken. It may also retain the service of such consultants or other persons that it considers are desirable.

5. The Commission shall be entitled to invite and consider submissions on such basis as it thinks appropriate.

5.2 *Definitions*

5.2.1 Accuracy

Noun 1. **accuracy** - the quality of nearness to the truth or the true value; "he was beginning to doubt the accuracy of his compass"; "the lawyer questioned the truth of my account"
truth
quality - an essential and distinguishing attribute of something or someone; "the quality of mercy is not strained"--Shakespeare
exactitude, exactness - the quality of being exact; "he demanded exactness in all details"; "a man of great exactitude"
fidelity - accuracy with which an electronic system reproduces the sound or image of its input signal
inaccuracy - the quality of being inaccurate and having errors

2. **accuracy** - (mathematics) the number of significant figures given in a number; "the atomic clock enabled scientists to measure time with much greater accuracy"
quality - an essential and distinguishing attribute of something or someone; "the quality of mercy is not strained"--Shakespeare
math, mathematics, maths - a science (or group of related sciences) dealing with the logic of quantity and shape and arrangement

Source: http://www.thefreedictionary.com

Webster Main Entry: **ac·cu·ra·cy**
Function: *noun*
Inflected Form(s): *plural* **-cies**
1 : freedom from mistake or error **: CORRECTNESS**
2 a : conformity to truth or to a standard or model **: EXACTNESS b :** degree of conformity of a measure to a standard or a true value -- compare PRECISION 2a

Webster Main Entry: **[2]correct**
Function: *adjective*
Etymology: Middle English, corrected, from Latin *correctus,* from past participle of *corrigere*
1 : conforming to an approved or conventional standard
2 : conforming to or agreeing with fact, logic, or known truth
3 : conforming to a set figure <enclosed the *correct* return postage>
- **cor·rect·ly**/ *adverb*
- **cor·rect·ness**/ *noun*
synonyms CORRECT, ACCURATE, EXACT, PRECISE, NICE, RIGHT mean conforming to fact, standard, or truth. CORRECT usually implies freedom from fault or error <*correct* answers> <socially *correct* dress>. ACCURATE implies fidelity to fact or truth attained by exercise of care <an *accurate* description>. EXACT stresses a very strict agreement with fact, standard, or truth <*exact* measurements>. PRECISE adds to EXACT an emphasis on sharpness of definition or delimitation <*precise* calibration>. NICE stresses great precision and delicacy of adjustment or discrimination <makes *nice* distinctions>. RIGHT is close to CORRECT but has a stronger positive emphasis on conformity to fact or truth rather than mere absence of error or fault <the *right* thing to do>.
Source: Merriam-Webster Online Dictionary

5.2.2 Testing

Noun 1. **testing** - the act of subjecting to experimental test in order to determine how well something works; "they agreed to end the testing of atomic weapons"
experiment, experimentation - the act of conducting a controlled test or investigation

2. **testing** - an examination of the characteristics of something; "there are laboratories for commercial testing"; "it involved testing thousands of children for smallpox"
examination, scrutiny - the act of examining something closely (as for mistakes)
screening - testing objects or persons in order to identify those with particular characteristics

3. **testing** - the act of giving students or candidates a test (as by questions) to determine what they know or have learned
examination
investigating, investigation - the work of inquiring into something thoroughly and systematically
11-plus, eleven-plus - (formerly in England) an examination taken by 11 and 12 year old students to select suitable candidates for grammar school

Source: http://www.thefreedictionary.com

Webster Main Entry: **test**
transitive senses
1 : to put to test or proof **: TRY**
2 : to require a doctrinal oath of
intransitive senses
1 a : to undergo a test **b :** to be assigned a standing or evaluation on the basis of tests <*tested* positive for cocaine> <the cake *tested* done>
2 : to apply a test as a means of analysis or diagnosis -- used with *for* <*test* for mechanical aptitude>
- **testability** / *noun*
- **testable** / *adjective*
- **test the waters** *also* **test the water :** to make a preliminary test or survey (as of reaction or interest) before embarking on a course of action

Source: Merriam-Webster Online Dictionary

5.2.3 Secrecy

Noun **1.** **secrecy** - the trait of keeping things secret
secretiveness, silence
uncommunicativeness - the trait of being uncommunicative
mum - secrecy; "mum's the word"

2. **secrecy** - the condition of being concealed or hidden
concealment, privateness, privacy
isolation - a state of separation between persons or groups
bosom - the chest considered as the place where secret thoughts are kept; "his bosom was bursting with the secret"
confidentiality - the state of being secret; "you must respect the confidentiality of your client's communications"

Source: http://www.thefreedictionary.com

Webster Main Entry: **se·cre·cy**

Function: *noun*
Inflected Form(s): *plural* **-cies**
Etymology: alteration of earlier *secretie*, from Middle English *secretee*, from *secre* secret, from Middle French *secré*, from Latin *secretus*
1 : the condition of being hidden or concealed
2 : the habit or practice of keeping secrets or maintaining privacy or concealment

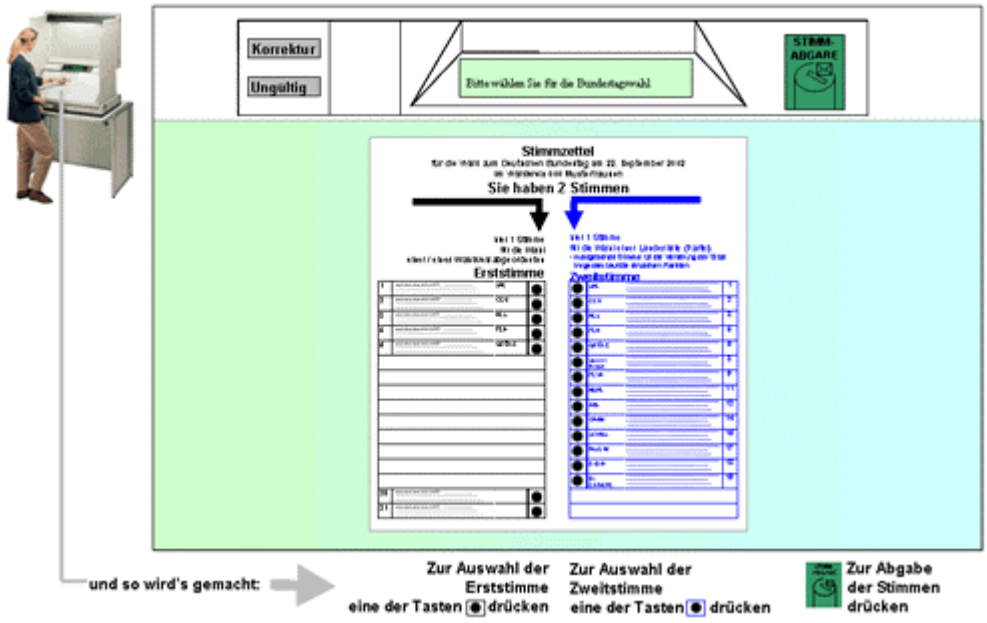
Source: Merriam-Webster Online Dictionary

6 Appendix B - Abstaining on Nedap machines

The question of intentionally spoiling ones vote has generated debate in Ireland. It is a fact that a measurable number of voters intentionally spoil their votes.

Whether such an action should be permitted in a democracy is a debate for another forum. Here we can agree that the current system allows for such actions so the new system should also allow for this.

The Nedap machine in Germany explicitly allows the voter to cast a void vote: See the website at http://www.wahlsysteme.de/



Note the second button at top left. It is labelled “ungultig”

A German translation offers the following:

English:	to declare **void**
German:	für ungültig erklären

It would be useful to confirm with Nedap if this in fact does allow the German voter to abstain.

The removal of this facility must have been a decision taken by the Minister or his Department.

In any case, it is a simple exercise to program the machine to permit a voter to abstain. The Irish voting machine has a spare button.

7 Appendix C - Joe McCarthy CV

52 Claremont Road, Sandymount, Dublin 4

Managing Director Arkaon Limited, network consulting company

Tel 01 660 4961 Fax 01 667 2208 Mobile 086 245 6788
Email joe.mccarthy at arkaon.com

BSc (UCG 1970)
Fellow, Irish Computer Society
Member, Marketing Institute of Ireland
Diploma in Legal Studies (DIT 1994)
Member, Internet Society
Chartered Engineer (IEI 2000)

Joe McCarthy is a consultant working in the network marketplace where he applies the latest technologies to the design and management of large-scale complex networks. He has substantial expertise in the telecommunications business - especially with regard to rapidly developing changes in technology and tariffs. His advice to clients enables them to achieve substantial cost reductions while improving overall service levels.

Joe has been working in the telecommunications and computer business in Ireland for over 30 years. His career in IBM Ireland gave him extensive experience in designing, marketing and implementing solutions for varied clients. These ranged from integrated re-engineering systems for Call Logging in Telecom Eireann's crossbar exchanges to the design of countrywide networks for large clients such as AIB and An Post.

He is a competent systems analyst and programmer. He is expert in programming languages including Fortran, Assembler, PL/1, Visual Basic and scripting languages. He is expert in database systems including Microsoft Access.

Joe spent a year as an Editor in IBM's International Systems Centre in London where he published 70 sets of books and manuals as part of the Large Systems Support Programme.

Joe was the Irish consultant for the Networking Practice of the IBM Consulting Group in his latter years with IBM, where he gained wide experience in network requirements analysis, technology selection, traffic & performance studies, and cost optimised design for large networks in Ireland and the UK. He left IBM in 1995 to set up his own consulting company.

Joe is now a consultant for Internet technologies, for data and voice integration systems and has provided advice on the regulatory position in the telecommunications market as it develops under the influence of EU directives. He has applied his skills and experience to reduce the cost and optimise the capacity of many nation-wide networks. Joe is a member of the Expert Group on Future Skills Needs which is

producing recommendations for government policy on the provision of sufficient skills for Ireland's growing economy.

He is interpreting the impact of the new networking technologies on their businesses for such diverse clients as Cablelink, Baltimore Technologies, Lifetime Assurance, the IMI, Údarás na Gaeltachta, the Department of Agriculture & Food, An Post and the National Lottery Company.

Projects completed by Arkaon include:

- Re-design and optimisation of a nation-wide network where technology change is facilitating dramatic reduction in cost while improving capacity and response. Technologies used include: IP, Dassnet, ATM, ISDN, PSTN, DWDM.

- Design, implementation and testing for a countrywide network of 3,500 POS terminals. Traffic measurement and reporting, transaction time optimisation, network cost management together with strategies to migrate legacy systems to an open standards platform.

- Design and implementation of a Public Key Infrastructure for a semi-state company. Disciplines addressed include IP planning, Firewall and resilience planning, development of PKI procedures for security and CPS.

- Design, coding and implementation of a network management platform based on Mapinfo which integrates SNMP, business data and trouble ticket reports for an office network of 1,000 locations.

- System design and implementation of a medium scale scanning and database project with some 100,000 documents per month being scanned and analysed. This system was based on NT and SQL Server with VB object modules to link the components from scanning to interpretation to database load to reporting. MS Access queries for trend analysis and quarterly reporting were also implemented.

- An interactive support environment for the LEADER II National Networking unit in Ireland. It includes databases, newsletters, reference material and discussion groups all built on a Lotus Domino server. It can be seen at http://www.leaderii.ie.

- Strategic analysis of the cryptographic marketplace for a client who purchased Baltimore Technologies. Subsequently ran a European test market campaign for their encryption products. Also planned and implemented the first Baltimore Web site.