Appendix 2A

Evaluation of Previous Testing – Part 1

THE POLICY INSTITUTE, TRINITY COLLEGE DUBLIN

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

Table of Contents

Glossary

DoEHLG	Department of the Environment, Heritage and Local Government
ERS	Electoral Reform Services Limited
IEC	International Electrotechnical Commission
IES	Integrated Election Software
LED	Light-Emitting Diode
KEMA	*NV tot Keuring van Elektrotechnische Materialen* (Electrical Engineering Equipment Testing Company)
PR-STV	Proportional Representation – Single Transferable Vote
PC	Personal Computer
PRU	Programming / Reading Unit
PTB	*Physikalisch-Technische Bundesanstalt* (Federal Physical and Technical Institute)
TCD	Trinity College Dublin
TNO	*Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek* (Netherlands Organisation for Applied Scientific Research)
VM	Voting Machine

Executive Summary

The ESI2/IES electronic voting system is comprised of two parts: a voting machine (ESI2) that voters use to cast their votes, and a PC application program (IES) that is used to prepare for an election and to count the results afterwards. A number of independent companies have been commissioned to test various aspects of the system. The voting machine has been tested by PTB, TNO, and Zerflow, and has been certified by KEMA. The entire IES has been desk-reviewed by Nathean, and the vote-counting part has been tested by ERS.

In assessing the "quality and comprehensiveness" of this testing, the report adopts the following approach:

- The voting process is divided into three stages (Pre-voting, Voting, and Post-voting), and each stage is further divided into a number of steps.
- Several key issues are identified for each step in the voting process. If these issues can be addressed satisfactorily, this will maximise confidence in the secrecy and accuracy of the proposed electronic voting system.
- In addressing each issue, the level of independent testing is examined and assessed. Instances of incomplete or inadequate testing are noted.

Based on the testing described in the independent test reports, the following conclusions are reached in this report:

1. The voting machine has been comprehensively tested.

2. The PRU has been neither independently tested nor desk-reviewed.

3. The vote-counting algorithm in the IES has been tested to an adequate standard.

4. The remainder of the IES has been desk-reviewed but has not been independently tested. Some of those features that have not been tested are very important to the election process, e.g. reading votes from ballot modules and aggregating votes at count centres.

5. No independent end-to-end testing has been performed.

1 Introduction

1.1 Objective of report

This report addresses Work Strand 2.a. of the research proposal by The Policy Institute (TCD) to the Commission on Electronic Voting [ref. 9]. Specifically, it addresses the proposal that "The computer science team will review previous reports on the proposed [electronic voting] system and write an evaluation of the quality and comprehensiveness of these".

The report is based on desk research and was prepared over the period 15 March 2004 to 13 April 2004.

Referenced documents are listed in Appendix A in alphabetical order.

1.2 Overview of testing undertaken

The proposed electronic voting system is the ESI2/IES system manufactured by the Dutch company Nedap N.V. It is comprised of two parts: a voting machine (ESI2) that voters use to cast their votes, and a PC application program (IES) that is used to prepare voting machines for an election and to count the results afterwards. (This document assumes that readers are familiar with the basic operation of the voting machine and IES – [ref. 3] contains a brief introduction.)

Both parts of the voting system have been tested by the manufacturer. (PTB [ref. 11, pp.51-52] has described the testing performed by Nedap on the voting machine.) In addition, a number of external companies have been commissioned to perform independent testing and checking of the system – see Table 1 for a summary.

This report examines the comprehensiveness and quality of these independent tests. Any shortcomings identified refer to the level of independent testing only, i.e. this report does not cover any testing performed by the manufacturer.

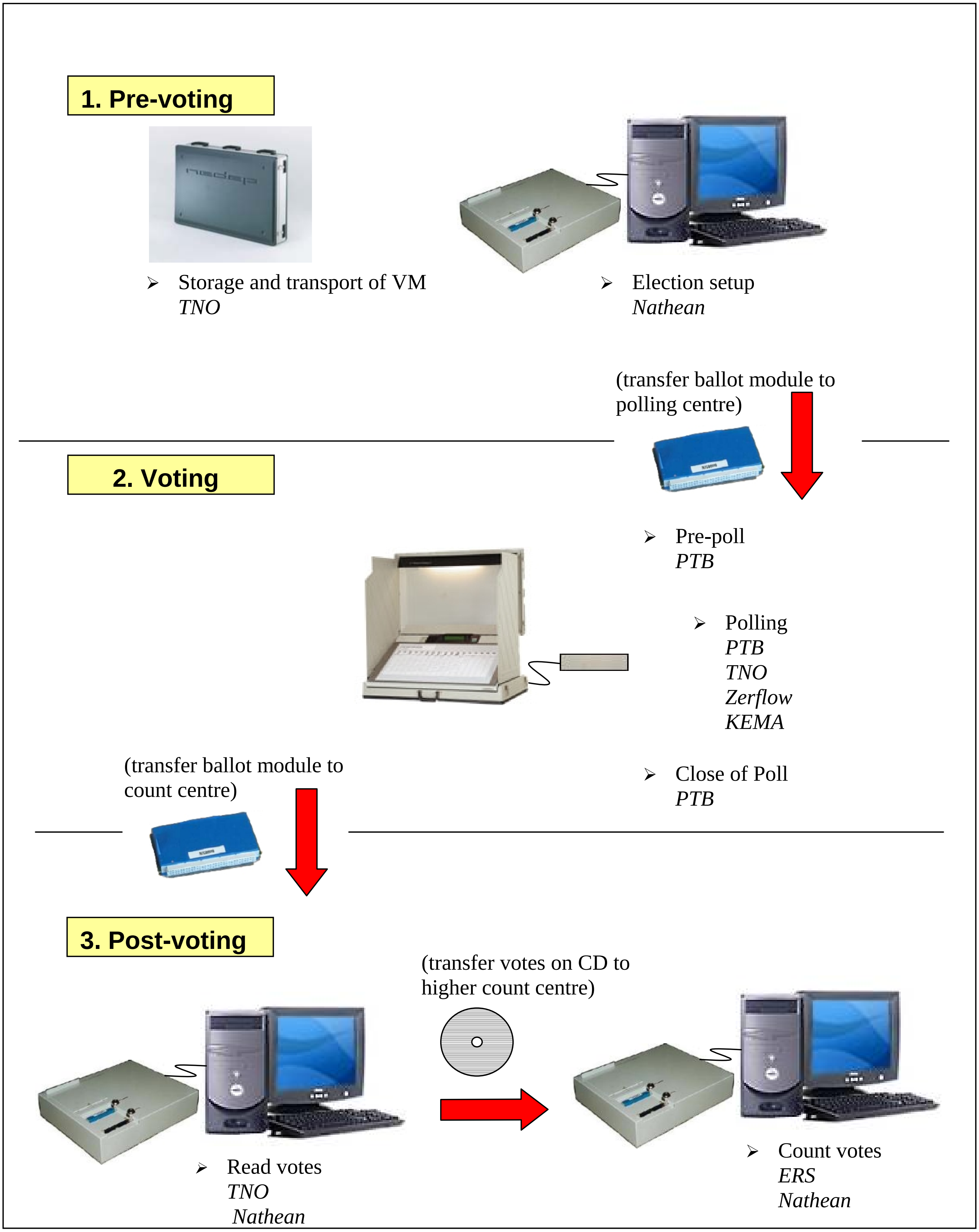
Table 1. Independent testing of the ESI2/IES voting system undertaken to date

Part of ESI2	**Testing Co.**	**Nature of Testing**
Voting Machine	PTB	Thorough testing of the functionality of voting machine (VM) hardware and software to verify that they meet their requirements [ref. 10, 11, 12, 13].
	Zerflow	Evaluation of the physical security of the VM [ref. 19, 20].
	TNO	Environmental testing of VM hardware to verify that it meets international standards in the following areas: temperature, humidity, interruptions to power supply, electromagnetic compatibility, insulation, energy consumption and transportation [ref. 14, 15, 16, 17, 18].
	KEMA	Certification that the VM hardware meets international standards [ref. 5].
IES	Nathean	Desk review of the entire IES [ref. 6, 7].
	ERS	Verification of the PR-STV count algorithms for Dáil, local and by-elections [ref. 4].

1.3 Steps in the electronic voting process

The main steps in the electronic voting process are shown in Figure 1 overleaf. The process is broadly divided into three stages: Pre-voting, Voting, and Post-voting. Figure 1 also shows the name of the company/companies whose independent testing is relevant for each step.

Fig. 1 Electronic Voting – 3 Main Stages



1. Pre-voting

- Storage and transport of VM
  TNO
- Election setup
  Nathean

(transfer ballot module to polling centre)

2. Voting

- Pre-poll
  PTB
- Polling
  PTB
  TNO
  Zerflow
  KEMA
- Close of Poll
  PTB

(transfer ballot module to count centre)

3. Post-voting

- Read votes
  TNO
  Nathean

(transfer votes on CD to higher count centre)

- Count votes
  ERS
  Nathean

1.4 Approach and method

In assessing the “quality and comprehensiveness” of previous testing, the approach used in this report is as follows:

- Each step in the voting process is examined and a number of key issues are identified. If these issues can be addressed satisfactorily, this will maximise confidence in the secrecy and accuracy of the proposed electronic voting system. The issues are selected on the basis that they encapsulate the core of the voting process; the list does not claim to be exhaustive.
- In addressing each issue, the level of independent testing is examined and assessed. Instances of incomplete or inadequate testing are noted.

The issues examined in this report are listed in Table 2.

Table 2. Key issues in the electronic voting process

Stage	*Step*	*Key Issue*
Pre-voting	Storage and transport of voting machines	1. Will voting machines function correctly after years in storage, and are they robust against accidental damage during transport? 2. Can voting machines be tampered with during storage, so that changes will be undetectable and will influence the outcome of subsequent elections?
	Election Setup	3. Can the IES and PRU be checked for authenticity? 4. Are steps taken to prevent unauthorised ballot modules and voting machines being used on Election Day? 5. Is election information (and only election information) reliably downloaded from the IES into ballot modules?
Voting	Pre-poll	6. Can it be confirmed that voting machines and ballot modules are functioning correctly before polling begins? 7. Can voting machines and ballot modules be checked for authenticity? 8. Can the electoral details stored on the ballot module be checked for accuracy?

Stage	*Step*	*Key Issue*
	Polling	9. Are voting machines physically secure against tampering? 10. Are voting machines protected against adverse environmental conditions? 11. Does the system ensure that each person can vote only once, and only in those polls in which he/she is entitled to vote? 12. Are the voter's preferences as displayed on the voter's panel accurately recorded in the machine's memory? 13. When the 'Cast Vote' button is pressed, are all preferences in memory accurately and reliably written to the ballot module? 14. Is the voting process secret? 15. Can a vote be lost if there is a power failure as the voter presses the Cast Vote button? 16. In the event of machine failure (for whatever reason), are all votes cast up until the point of failure secure?
	Close of poll	17. Can voting machines and ballot modules be checked to ensure that no tampering has taken place during the day? 18. Is the primary ballot module accurately copied to the backup module at close of poll? 19. Is it certain that no additional votes can be added to a ballot module after close of polling?
Post-voting	Reading of votes	20. Can ballot modules be authenticated to ensure that they are genuine? 21. Does the IES accurately read all votes from each ballot module? 22. In the case of multiple polls, is the system of transferring votes to a different count centre reliable and secure? 23. Are votes from different ballot modules correctly aggregated?
	Counting of votes	24. Are all votes randomly mixed prior to counting? 25. How reliable is the PR-STV counting software?

1.5 Structure of report

There are five further sections in this report:

- Section 2 examines key issues at the Pre-voting stage (Issues 1-5).
- Section 3 examines key issues during the Voting stage (Issues 6-19).
- Section 4 examines key issues at the Post-voting stage (Issues 20-25).
- Section 5 summarises the findings of this report.
- Section 6 comments on the overall quality and comprehensiveness of independent testing.

For each key issue highlighted in Sections 2, 3 and 4, the companies that performed the relevant independent testing are identified, and the comprehensiveness and quality of their testing is evaluated. These terms have been interpreted as follows in this report:

Comprehensiveness: Was the scope of the independent testing sufficiently broad? i.e. are there parts of the system that have not been tested?

Quality: Was the independent testing sufficiently thorough? i.e. for each part of the system that has been tested, does the testing give a high degree of confidence that it will function correctly during operation?

The evaluation of testing for each function takes into account the function's importance in producing an accurate election result, and also considers whether its correctness can be confirmed with manual checks. Higher standards of testing are expected for vital functions and for those whose correct operation cannot be verified by manual procedures.

It is assumed that the testing documented by each company has in fact been carried out fully and to a high standard. This report did not review internal test documentation showing *how* the tests were performed, but is based on the test result summaries supplied by each company.

2 Evaluation of testing: pre-voting

2.1 Overview

Pre-voting includes all activities carried out before Election Day. It includes storage and transport of voting machines, and election preparation using the IES.

2.2 Storage and transport of voting machines

Issue 1: Will voting machines function correctly after years in storage, and are they robust against accidental damage during transport?

<u>Comment on Issue 1</u>
The manufacturer of the voting machines, Nedap, has stated "no maintenance is required during storage" [ref. 2, p. 31].

The effect of prolonged periods of storage on voting machines has not been tested directly. However, TNO [ref. 14-18] has tested a number of limiting conditions for storage and transport of voting machines, and has found them to be resistant to vibration and shock, electromagnetic interference, dripping water, and extremes of temperature and humidity. (The range of environmental conditions that voting machines must withstand is listed in [ref. 10, pp.16-17].)

During the 1998 national elections in the Netherlands, 23 out of 5,128 (0.44%) machines failed, 18 of which were replaced before polling started [ref. 2, p.21]. No failures (0 out of 600) were recorded in Cologne when ballot modules were installed before machines were dispatched to polling places.

Conclusion on Issue 1

Comprehensiveness of Testing:	Tolerance of voting machines to a wide range of environmental conditions during storage has been tested by TNO.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 2: Can voting machines be tampered with during storage, so that changes will be undetectable and will influence the outcome of subsequent elections?

Comment on Issue 2

Voting machine hardware, backup ballot module, and voting machine software can be considered separately.

The voting machine's hardware uses standard electronic components but uses printed circuit boards of non-standard dimensions. This means that replacement boards would have to be specially constructed for the purpose. Any hardware malfunction is detected by the machine's software during operation – this has been tested by PTB [ref. 11, pp.7-10, p.43].

The backup ballot module remains in the machine at all times. PTB [ref. 11, p.32] has verified that before the contents of the primary module are copied into it at close of polling, all data on the backup module is automatically erased.

Might it be possible to tamper with a voting machine's software? The answer is that this is theoretically possible. Someone with access to Nedap's source code (written in C) could alter the program while also ensuring that it returned the expected checksum at start-up. One possible alteration, for example, would be to enable a voter to press buttons in a specific sequence during polling that would cause the machine to alter preferences in favour of a particular candidate from that point on. The danger that machine software can be altered is explicitly highlighted by PTB [ref. 11, p.11]: "an exchange of the ROM chips including fraudulent presentation of the correct checksums cannot be avoided by software but by means of sealing only".

Conclusion on Issue 2

Comprehensiveness of Testing:	PTB has verified that tampering with voting machine hardware or the backup ballot module will either have no effect or else will be detected during operation. There are no tests that would detect fraudulent exchange of voting machine software; this may be avoided by secure storage of voting machines between elections.

Quality of Testing:	Adequate.

2.3 Election set-up

Issue 3: Can the IES and PRU be checked for authenticity?

Comment on Issue 3
Apart from a few differences, the PRU and voting machine use the same hardware [ref. 8, p.51]. PRU software is therefore stored in the same way as voting machine software, i.e. it is burned into two EPROM chips [ref. 10, p.6].

IES software runs on a 'hardened PC'. It is stored on CD, and the correct version to use is specified by Ministerial Order prior to each election [ref. 1, p.7].

Is it possible to verify that the correct versions of PRU and IES software are being used at any moment, and that unauthorised personnel have not tampered with the software? Malicious changes to PRU software, for example, might allow votes to be altered while being read from ballot modules after an election. Malicious changes to the IES software used for mixing votes prior to counting, for example, might allow a particular party/candidate to be unduly favoured by transfers during the count.

It does not appear to be possible to verify the authenticity of PRU and IES software.

Voting machine hardware and software are validated by comparing checksums calculated at start-up with those supplied in printed documentation (see Issue 7). These checks do not seem to be available for the IES or PRU; the IES version and build number can be displayed, but this does not guarantee that the software is authentic. Since these checks are not available, they could not be independently tested.

Conclusion on Issue 3

Comprehensiveness of Testing:	**The IES and PRU cannot be checked for authenticity, so no testing has been carried out for this issue.**
Quality of Testing:	Not applicable.

* * * * * * * * * *

Issue 4: Are steps taken to prevent unauthorised ballot modules and voting machines being used on Election Day?

Comment on Issue 4
Yes. According to the DoEHLG [ref. 1, p. 8], "when a ballot module has been programmed … the IES records the serial number of the module in the system along with the relevant polling station for security checking upon return of the module after the poll has closed". So a ballot module will not be read at the end of Election Day if:
a) Its module ID is not in the list of those officially programmed for the election, or
b) It has been used in the wrong polling station.

This aspect of the IES has been desk-reviewed by Nathean [ref. 7], but does not appear to have been independently tested.

Conclusion on Issue 4

Comprehensiveness of Testing: Nathean has carried out a full desk-review of the relevant IES software.

Quality of Testing: Nathean desk-review is adequate. **However, it is very important that no unauthorised ballot modules can be introduced on Election Day. The security and correctness of the IES in this regard have not been independently tested. (See also Issue 20)**

* * * * * * * * * *

Issue 5: Is election information (and only election information) reliably downloaded from the IES into ballot modules?

Comment on Issue 5

According to the DoEHLG, [ref. 1, p.8], “a print-out is made to verify that the details loaded in the ballot module are the same as those approved by the returning officer concerned”. So the election information on the ballot module can be manually confirmed. The software involved has also been desk-reviewed by Nathean [ref. 7].

Can ballot modules be used to transfer other data to voting machines that will influence their behaviour during Election Day? PTB [ref. 11, pp.16-17] has listed all items in the ballot module that are checked at machine start-up. It does not state whether there is space in the module for additional information, however, and does not specifically rule out the possibility that additional data can be passed from PC to voting machine – this was not one of its testing requirements [ref. 12]. (PTB’s 1998 report on the ESD-1 voting machine used in German elections [ref. 13, p.31] does address this point directly: “There is no basis to assume that inadmissible data or information is transferred from the IES to the voting machine via the storage module. There is no executable code in the storage modules which can affect the functioning of the voting machine, only data which is described in the documentation and whose use can be well understood using the source text”. It is not known whether this conclusion also applies to the Irish ESI2 machine.)

Conclusion on Issue 5

Comprehensiveness of Testing: **Download of election information from IES to ballot module can be checked using manual procedures. It has not been verified that there is no possibility to transfer ‘extra’ data from IES to ESI2 via the ballot module.**

Quality of Testing: Nathean desk-review is adequate.

3 Evaluation of testing – voting

3.1 Overview

The voting stage covers all activities from the moment ballot modules are placed into voting machines until the end of polling. It can be divided into three parts: pre-poll, polling, and close of poll.

3.2 Pre-poll

Issue 6: Can it be confirmed that voting machines and ballot modules are functioning correctly before polling begins?

Comment on Issue 6
Yes. Voting machines perform extensive self-testing after being switched on, and will shut down if a problem is detected. This has been confirmed by PTB [ref. 11, pp. 7-10]. The primary ballot module is also checked, and will be blocked if it contains invalid or inconsistent data [ref. 11, pp.16-17]. Note that this check does not confirm that stored information is correct – see Issue 8 below.

Conclusion on Issue 6

Comprehensiveness of Testing:	Start-up checks on voting machine and ballot module have been tested by PTB.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 7: Can voting machines and ballot modules be checked for authenticity?

Comment on Issue 7
Yes, voting machines and ballot modules can be checked by election staff using the printed 'open poll statement'. This has been verified by PTB [ref. 11, p.15]: "The voting machine is identified by its machine ID and the hardware versions. The software is identified by the software versions and checksums. The ballot module is identified by its module ID. All these identification terms cannot be changed during voting process. They are typed out without modifications." Election staff must manually match all identification numbers and checksums against those provided in printed documentation.

Conclusion on Issue 7

Comprehensiveness of Testing:	Printing of IDs for voting machine hardware, ballot modules and software has been tested by PTB. Checking of IDs is performed using manual procedures.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 8: Can the electoral details stored on the ballot module be checked for accuracy?

Comment on Issue 8
Yes. PTB [ref. 11, pp.17-18] has verified that election data from the ballot module can be printed out at start-up in the 'open poll statement'. This data includes details of each poll, candidate details, and identifies which buttons should be active on the voting machine's panel [ref. 11, pp.16-17]. A thorough manual check of this information should catch any problems that occur during election set-up. Every button on the voter's panel should also be checked using the machine's test procedures [ref. 8, p.40]. Each candidate's button, when pressed, should result in the candidate's

name appearing in the voter display. No other buttons should be programmed. Finally, the printed statement should indicate that no votes have already been cast in any of the day's polls.

Conclusion on Issue 8

Comprehensiveness of Testing:	PTB has tested that the 'open poll statement' is printed correctly. Election staff must manually verify election details.
Quality of Testing:	Adequate.

Note: the automatic and manual checks carried out during the pre-poll period appear to catch almost every possible error or inconsistency that may have been introduced up to this point. Once all checks have been passed, then based on the literature, it is possible to have a high degree of confidence that all parts of the electronic voting system are operating correctly.

3.3 Polling

Issue 9: Are voting machines physically secure against tampering?

Comment on Issue 9

Yes. Voting machines are physically sealed so that any interference with the internal electronics or the ballot module can be detected [ref. 1, p.9]. They are also positioned in plain view of voting staff throughout the day. The voter's panel on each machine is locked so that ballot papers cannot be exchanged [ref. 20, p.1], and will be periodically checked by election staff throughout the day to ensure that it has not been tampered with or defaced [ref. 1, p.12]. These procedures have been reviewed and approved by Zerflow, which concluded, "the voting machine is now secure" [ref. 20, p.2].

Conclusion on Issue 9

Comprehensiveness of Testing:	Zerflow has verified that voting machines are physically secure during polling.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 10: Are voting machines protected against adverse environmental conditions?

Comment on Issue 10

Yes. Environmental conditions can change naturally or as the result of a deliberate attempt to disrupt a voting machine's operation. Voting machines must be tolerant to a wide range of environmental conditions – the requirements are listed in [ref. 10, pp.16-17]. They include tolerance to fluctuations in power, humidity and temperature; to physical shock and vibration; to dripping water; and to electromagnetic radiation. Voting machines were successfully tested against these requirements by TNO [ref. 14, 15, 16, 17, 18].

An important question is whether the votes stored in a ballot module might be erased by a strong magnetic field. To test this, the Policy Institute exposed a populated ballot module to a magnetic field of 7 Teslas. Data on the module was unaffected.

Conclusion on Issue 10

Comprehensiveness of Testing: A range of environmental tests has been carried out by TNO.

Quality of Testing: Adequate.

* * * * * * * * * *

Issue 11: Does the system ensure that each person can vote only once, and only in those polls in which he/she is entitled to vote?

Comment on Issue 11

Yes. The polling card system is unchanged under electronic voting, so the question is whether each voter who presents a valid polling card is allowed to cast one vote only. PTB [ref. 11, pp.21-22] confirms that election staff can select which polls a voter is allowed to vote in using the voting machine's control unit. After each vote is stored, the software automatically deactivates all keys on the voter's panel. No further votes can be cast until a member of the election staff reactivates the machine using the control unit [ref. 11, pp.27-28].

Conclusion on Issue 11

Comprehensiveness of Testing: PTB has tested that only one vote is stored per machine activation. Election staff must ensure that the correct polls are active for each voter.

Quality of Testing: Adequate.

* * * * * * * * * *

Issue 12: Are the voter's preferences as displayed on the voter's panel accurately recorded in the machine's memory?

Comment on Issue 12

As each voter presses buttons on the voting machine's panel, a list of preferences for each poll is constructed in the machine's memory [ref. 11, p.23]. The question is whether the displayed preferences and the internal lists are always an accurate reflection of one another.

This seems to be assured by the manner in which the display function is implemented. The lists of preferences stored in memory are the 'master copy' and the LEDs on the voter's panel reflect this stored information [ref. 11, pp.23, 25]. The voter's only options are to select a new preference or reselect an old one; both have been tested and validated by PTB. Note that if a button stops working during polling (so that pressing it has no effect), it is up to the voter to bring this to the attention of election staff.

Conclusion on Issue 12

Comprehensiveness of Testing: PTB has verified that the internal representation of displayed preferences is correct.

Quality of Testing: Adequate.

* * * * * * * * * *

Issue 13: When the 'Cast Vote' button is pressed, are all preferences in memory accurately and reliably written to the ballot module?

Comment on Issue 13

Yes. PTB [ref. 11, p.27] has verified that once the 'Cast Vote' button has been pressed, the storage process cannot be interrupted by the voter or election staff, but only by major hardware faults.

The security of stored votes has also been comprehensively tested [ref. 11, p.10, pp.26-27, 33-35, 37-39]. Each vote is stored twice in each of the two independent memory chips within the ballot module. All four copies are stored together with a Hamming code, and two of the four are inverted. Each time a single vote is read, all four copies are read. In the unlikely event of a storage failure, an error code will be displayed on the control unit [ref. 11, pp.38-39]. The voter should then be able to vote again (using a different machine).

Conclusion on Issue 13

Comprehensiveness of Testing:	PTB has tested that votes are stored reliably in the ballot module.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 14: Is the voting process secret?

Comment on Issue 14

This question has two parts.

First, can a voter's preferences be seen during or after the voting process? The answer is no. PTB [ref. 11, p.30] has confirmed that preferences are not displayed on the voting machine's control unit, and therefore cannot be seen by election staff. It also found [ref. 11, p.29] that after the 'Cast Vote' button has been pressed, all LED's next to voter's preferences are switched off and the machine's display is cleared.

Second, can a voter be identified from the position of his/her vote in the ballot module? Again, the answer is no. Votes are stored randomly in the voting module, so that even someone with knowledge of the storing method cannot predict where votes are located [ref. 11, p.40].

Conclusion on Issue 14

Comprehensiveness of Testing:	PTB has verified that the voting process is secret. Note that there is no requirement that voters should be able to spoil their votes in secret, and so this has not been tested.
Quality of Testing:	Adequate

* * * * * * * * * *

Issue 15: Can a vote be lost if there is a power failure as the voter presses the Cast Vote button?

Comment on Issue 15

No. If mains power fails on Election Day, each voting machine will have battery backup and will be able to continue functioning without interruption [ref. 11, p.36]. If the battery fails too, then a number of situations can occur. If the current voter has not pressed the 'Cast Vote' button, he/she can be allowed to vote using a different machine. If the 'Cast Vote' button has been pressed, the control unit operator must wait until power has been restored and then check whether the number of votes for each poll has increased by one [ref. 11, p.35].

The various scenarios involved have been tested by PTB [ref. 11, pp.44-45]. Its conclusion is that no permanent harm can be caused to the system by power failure. Election staff will always be able to determine whether a vote was stored or not once power has been restored.

Conclusion on Issue 15

Comprehensiveness of Testing: PTB has verified that a vote cannot be lost because of a power failure (assuming power subsequently returns). **The test documentation does not, however, explain what happens if power fails while a vote is being stored in the ballot module, e.g. 2 of the 4 write operations have been completed, and the 3rd is underway. It needs to be clarified whether this is possible, and whether it might corrupt the module's vote memory.**

Quality of Testing: Adequate.

* * * * * * * * * *

Issue 16: In the event of machine failure (for whatever reason), are all votes cast up until the point of failure secure?

Comment on Issue 16

Yes. This has been confirmed by PTB [ref. 11, p.11]: "erasure of data is physically impossible as long as the ballot module is inside its slot and only programming voltage is used". PTB also confirmed that data is only written to the ballot module at the end of the voting process for each voter, and that nothing is written if the memory space is already occupied [ref. 11, p.36]. So previous votes cannot be overwritten by mistake. Additional physical measures "inhibit deletion or complete overwriting of votes", although these should not be needed.

Conclusion on Issue 16

Comprehensiveness of Testing: PTB has verified that stored votes are secure if a voting machine fails.

Quality of Testing: Adequate.

3.4 Close of poll

Issue 17: Can voting machines and ballot modules be checked to ensure that no tampering has taken place during the day?

Comment on Issue 17

Yes. The security of the primary and backup ballot modules and of the voting machine's hardware and software are protected throughout the day by a physical seal. In addition, the printed 'close polling statement' [ref. 8, p.37] contains details of the machine, ballot module, election, and candidates. PTB [ref. 11, pp.30-31] has verified that this is printed correctly. Election staff must verify that these details match the printed 'open poll statement' produced before polling began.

Conclusion on Issue 17

Comprehensiveness of Testing:	PTB has verified that the 'close polling statement' is printed correctly. Verifying that a machine has not been tampered with is performed manually.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 18: Is the primary ballot module accurately copied to the backup module at close of poll?

Comment on Issue 18

The poll can be closed in two ways, and both involve creating a backup of the primary ballot module [ref. 8, p.35]. PTB [ref. 11, p.32] has confirmed that the entire contents of the backup module are always deleted before the backup is made. It has not tested that the contents of the primary and backup modules are identical after the backup procedure. This was not included in its test requirements [ref. 12], perhaps because the backup copy has never been needed – when asked what would happen "in the event of a cartridge/disc being lost or destroyed before it is entered in counting system" [ref. 2, p.28], Nedap replied that "in all our accumulated experience of over 25.000 machines in use such a situation has never occurred". Nevertheless, it is important to be sure that the backup procedure does indeed produce an identical copy of the primary ballot module.

Conclusion on Issue 18

Comprehensiveness of Testing:	PTB has verified that the contents of the backup module are deleted prior to the backup being made. **It has not been tested that the backup is an exact copy of the primary ballot module**.
Quality of Testing:	Adequate.

* * * * * * * * * *

Issue 19: Is it certain that no additional votes can be added to a ballot module after close of polling?

Comment on Issue 19

Yes. The ESI2 function specification [ref. 8, p.14] states: "the primary ballot module is blocked by the voting machine software at the close of poll so that it is not possible to store more votes in it". This is confirmed by PTB [ref. 11, p.32]. Closing the poll sets a flag in the ballot module that "is not erasable without the complete module being erased".

Conclusion on Issue 19

Comprehensiveness of Testing:	PTB has verified that additional votes cannot be added to a ballot module after close of polling.
Quality of Testing:	Adequate.

4 Evaluation of testing: post-voting

4.1 Overview

The post-voting stage begins with the arrival of ballot modules at the count centre. It includes reading, aggregation, and counting of votes using the IES.

4.2 Reading of votes

Issue 20: Can ballot modules be authenticated to ensure that they are genuine?

Comment on Issue 20

Yes. During election set-up, the identities of all primary ballot modules to be used on Election Day are recorded in the IES (see Issue 4). When the first vote is stored in a ballot module during polling, "the identification of the voting machine is written into the module information area of the ballot module. So it is always known on which voting machine the ballot module was used for voting" [ref. 11, p.33].

The DoEHLG [Ref. 1, p.14] has described what happens when a module arrives at a count centre after close of polling: "before the module is accepted, the system verifies that it is a module programmed for the poll and for the correct polling station". A ballot module will not be read if it has an invalid ID or if it has been used in the wrong polling station. This has been verified by Nathean [ref. 7] in a desk-review of the software involved.

Is there a possibility that two ballot modules could be programmed to have the same module ID? Could they then be switched without the system detecting that anything was wrong? This was considered by PTB [ref. 11, p.4]. It found that the voting machine software does not overwrite the module ID at any time. The module ID can only be changed when the hardware is configured as a PRU in Service mode, and only after the module has been completely erased. (The system can be placed in Service mode "either by manually turning a DIPswitch on the main electronic board or by inserting a 'SERVICE' ballot module with a special ID" [ref. 8, p.48].)

So theoretically, it would be possible to program two ballot modules with the same ID. Any voting machine could be used to enter votes on the duplicate module prior to Election Day. Someone could then exchange modules either before the 'close polling statement' was printed (this would involve breaking the seal), or else exchange both module and statement en route to the count centre. Either action would be uncovered by comparing the number of voters counted manually by election staff with the number printed on the 'close polling statement'.

Conclusion on Issue 20

Comprehensiveness of Testing:	Nathean has desk-reviewed all relevant parts of the IES. Manual procedures must be used to avoid the possibility that duplicate modules (i.e. modules with the same ID as authentic modules) are introduced.
Quality of Testing:	The Nathean desk-review is adequate. **However, no independent testing has been performed to confirm that unauthorised ballot modules will not be read.**

* * * * * * * * * *

Issue 21: Does the IES accurately read all votes from each ballot module?

<u>Comment on Issue 21</u>
When a ballot module arrives at a count centre, it is inserted in a PRU's reading slot and read into a PC using the IES.

IES software for this function has been desk-reviewed by Nathean [ref. 7], but the PRU's role does not appear to have been independently tested. (The tolerance of PRU hardware to environmental conditions has been tested by TNO [ref. 17, 18], but the PRU's read/write functionality has not been desk-reviewed or tested.)

The DoEHLG [Ref. 1, p.14] has stated that the number of votes read from a ballot module for each poll is manually compared with the number printed out in the 'close polling statement'. So it can be verified on polling day that no votes are lost in the reading process.

<u>Conclusion on Issue 21</u>
Comprehensiveness of Testing: The relevant IES software has been desk-reviewed by Nathean. However, **the PRU's role in the reading procedure has not been independently tested or desk-reviewed**.

Quality of Testing: Nathean's desk-review is adequate. **However, it is critical to the election process that votes are not inadvertently altered while being read. The system does not appear to provide a mechanism to check this. (For example, the voting machine might have printed a checksum for each poll on the 'close polling statement', and this could have been independently re-calculated by the IES and manually checked.) Given the importance of the reading function and the fact that its correct operation cannot be manually verified, this may represent a gap in the independent testing.**

* * * * * * * * * *

Issue 22: In the case of multiple polls, is the system of transferring votes to a different count centre reliable and secure?

<u>Comment on Issue 22</u>
The DoEHLG [Ref. 1, p.14] has explained the procedure for transferring votes to a higher count centre during a multi-poll election: data is encrypted, burned onto a CD-R, and delivered by hand together with a paper reconciliation record.

Nathean has desk-reviewed the relevant parts of the IES. No independent testing appears to have been carried out to verify that this transfer method is completely reliable.

Conclusion on Issue 22

Comprehensiveness of Testing: Nathean has desk-reviewed the relevant IES software. **However, it is important to be sure that data cannot be corrupted or lost during the transfer procedure. Other hardware and software are involved besides the IES, e.g. to write data to CDs. These elements have not been independently tested, nor has the transfer procedure as a whole.**

Quality of Testing: Nathean desk-review is adequate, but **the IES function for transferring votes between count centres has not been independently tested.**

* * * * * * * * * *

Issue 23: Are votes from different ballot modules correctly aggregated?

Comment on Issue 23

Yes. This function has been desk-reviewed by Nathean [ref. 7], but again, has not been independently tested.

In its security audit, the DoEHLG [Ref. 1, p.15] appears to state that after all votes in a particular poll have been aggregated, the total number of votes is verified against the numbers in individual statements. So when the count is carried out on the same PC that was used to read in votes from individual ballot modules, the total number of aggregated votes must be equal to the combined total from all ballot modules. When the count is carried out at a higher count centre, the total number of aggregated votes must equal the total from all CDs. Either way, this manual procedure will verify that no votes have been lost.

Conclusion on Issue 23

Comprehensiveness of Testing: Nathean has desk-reviewed the relevant parts of the IES.

Quality of Testing: Nathean desk-review is adequate. **However, it is important to have confidence that no votes are changed during the aggregation process. The system does not seem to provide a mechanism to verify this during operation (see Issue 24 for an example of how it might have been done). Therefore, the only way to verify that the aggregation function operates correctly is through prior testing. No independent testing of the aggregation function has been performed.**

4.3 Counting of votes

Issue 24: Are all votes randomly mixed prior to counting?

Comment on Issue 24

Since the electronic voting system imitates the system used for manual counting, it is necessary to mix votes before running the count algorithm. Votes are numbered sequentially after being mixed. If a surplus arises during the count, those votes with higher index numbers are transferred. The final result could be distorted by non-random mixing if lower preferences for certain candidates received higher index numbers – those candidates might then receive a higher proportion of transferred votes than others.

The DoEHLG [Ref. 3, p.9] has explained that the IES "utilises a widely used computer algorithm called the Lehmer algorithm", seeded with a value from the system clock. This algorithm will produce a random mixing of votes. The software has been desk-reviewed by Nathean [ref. 7].

Conclusion on Issue 24

Comprehensiveness of Testing: Software for this function has been desk-reviewed by Nathean.

Quality of Testing: Desk-review is adequate. But as with Issues 22 & 23, **it is important for the election process that votes are not altered during the mixing process. Again, there is no evidence that the system includes a mechanism to check this during operation**. (One way to verify that aggregated and mixed votes are the same as those read in from ballot modules/CDs would be as follows: 1.Create a copy of the file containing the aggregated & mixed votes. 2.Scan through the votes from each ballot module/CD. As each individual vote is read, remove it from the file created in step 1. 3.At the end of this procedure, verify that this file is empty.) **The correctness of the mixing process therefore relies on system testing. However, the function has not been independently tested.**

* * * * * * * * * *

Issue 25: How reliable is the PR-STV counting software?

Comment on Issue 25

ERS [ref. 4] has tested Nedap's implementation of the Irish PR-STV counting algorithm for general, local and by-elections. The method it used was to implement the algorithm independently, and to compare its output with Nedap's over a range of test cases. The test report includes a full list of all test cases that were run. It concludes, "the risk of IES v121 producing an incorrect result sheet in an actual election is less than 1 in 1,000 cases, but perhaps not less than 1 in 10,000 cases" [ref. 4, p.7].

Conclusion on Issue 25

Comprehensiveness of Testing: ERS ran a total of 425 test cases for general, local and by-elections, with an extra 9 for by-elections only (total: 1284 tests). These include a range of normal and unusual cases.

Quality of Testing: The number of potential test cases for the count algorithm is extremely large. ERS concedes: "we suspect that if it were practical to run several thousand, rather than several hundred, test cases through IES, then we might find an error" [ref. 4, p.7]. **When The Policy Institute research team attempted to run test cases through IES, it found that the interface to the count algorithm was both slow and awkward. If a**

quicker interface were available, it would be relatively straightforward to automatically generate and execute thousands of additional test cases. This would increase confidence in the correctness of the count algorithm.

5 Summary of findings and points arising

5.1 Summary of findings

Table 3 summarises the findings of this report regarding the quality and comprehensiveness of independent testing across 25 key issues in the election process (listed in Table 2). These issues were identified on the basis that addressing them would maximise confidence in the secrecy and accuracy of the electronic voting system.

All points arising are discussed in Section 5.2.

Table 3. Summary of findings[1]

Stage	*Step*	*Key Issue*	*Test Comprehensiveness*	*Test Quality*	*Point*
Pre-voting	Storage and transport of VMs	1. 2.	Adequate Adequate	Adequate Adequate	
	Election Set-up	3. 4. 5.	No testing possible Adequate Not fully covered	N/A Desk-reviewed only Adequate	1 2 3
Voting	Pre-poll	6. 7. 8.	Adequate Adequate Adequate	Adequate Adequate Adequate	
	Polling	9. 10. 11. 12. 13. 14. 15. 16.	Adequate Adequate Adequate Adequate Adequate Adequate Clarification needed Adequate	Adequate Adequate Adequate Adequate Adequate Adequate Adequate Adequate	4
	Close of poll	17. 18. 19.	Adequate Not fully covered Adequate	Adequate Adequate Adequate	5
Post-voting	Reading of votes	20. 21. 22. 23.	Adequate Not fully covered Not fully covered Adequate	Desk-reviewed only Desk-reviewed only Desk-reviewed only Desk-reviewed only	6 7 8 9

[1] The meanings of the terms 'Test Comprehensiveness' and 'Test Quality' are given in Section 1.5.

Stage	*Step*	*Key Issue*	*Test Comprehensiveness*	*Test Quality*	*Point*
	Counting of votes	24. 25.	Adequate Adequate	Desk-reviewed only More testing possible	10 11

5.2 Points arising

Based on the desk research undertaken for this report on the independent testing of the ESI2/IES electronic voting system, a number of points arise. These 11 points relate to possible gaps in the independent testing, or areas where the level of testing might have been more thorough. The points (and the issues to which they link) are as follows:

1. (Issue 3) The system does not seem to provide a means of checking that PRU and IES software are authentic. This has therefore not been tested.

2. (Issue 4) The IES function for registering ballot modules prior to Election Day has not been independently tested.

3. (Issue 5) It has not been verified that hidden information cannot be passed from the IES to the voting machine via the ballot module.

4. (Issue 15) Is it possible that, while a vote is being written to the ballot module, a power failure might lead to corruption of the vote memory? This point can be clarified with PTB.

5. (Issue 18) Following the backup procedure at close of poll, does the backup module contain an exact copy of information on the primary ballot module? PTB may be able to answer this.

6. (Issue 20) The IES function for verifying the authenticity of ballot modules before reading in votes has not been independently tested.

7. (Issue 21) This function for reading votes from ballot modules has not been tested to ensure that votes are always read accurately.

8. (Issue 22) The reliability of transferring votes between count centres has not been verified.

9. (Issue 23) The IES function for aggregating votes from multiple CDs/ballot modules has not been independently tested.

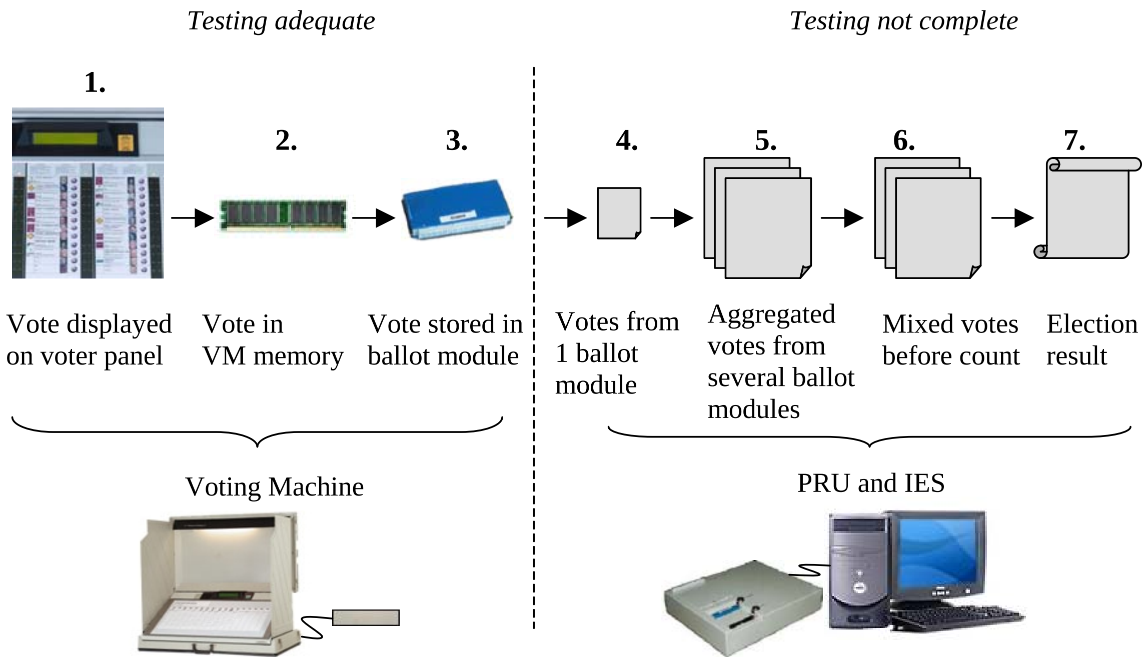
10. (Issue 24) Mixing of votes prior to counting has not been independently tested.

11. (Issue 25) Additional testing of the PR-STV count algorithm would increase confidence in its correctness.

6 Comment on findings

This report has assessed the comprehensiveness and quality of independent (i.e. non-manufacturer) testing for a range of issues that arise in the electronic voting process. In order to comment on the overall comprehensiveness and quality of testing, it will help to focus on the core of the process as shown in Figure 2 below.

Fig 2. Electronic Voting – Tracking a Single Vote



This figure tracks a single vote through the system from the time it is entered by the voter until the election result has been calculated. It highlights the central issues in the electronic voting process:

1. Does the voter's panel correctly display the voter's preferences?
2. Are the voter's preferences as displayed on the voter's panel accurately reflected in the voting machine's memory?
3. When the voter presses the 'Cast Vote' button, are votes accurately and reliably written to the ballot module?
4. Are votes accurately read from a ballot module into the IES?
5. Are votes correctly aggregated at the count centre?
6. Are votes correctly and randomly mixed prior to counting?
7. Are votes accurately counted in accordance with PR-STV?

Figure 2 also shows that the independent testing is broadly adequate for the first three of these issues (involving the voting machine), but that there are some gaps in the independent testing for the remaining four (involving the PRU and IES).

When combined with the detailed findings outlined in Section 5, Figure 2 leads to the following conclusions regarding the overall quality and comprehensiveness of the independent testing:

1. The voting machine has been comprehensively tested to a high standard, in particular by PTB and TNO.

2. The PRU has been neither independently tested nor desk-reviewed.

3. The IES count software has been tested to an adequate standard by ERS. Additional testing would increase confidence in the accuracy of the software.

4. The remainder of the IES has been desk-reviewed by Nathean, but has not been independently tested. Desk-reviews are generally not an adequate alternative to testing for a large piece of software such as the IES, and additional testing is therefore desirable.

5. No independent end-to-end testing has been carried out on the system. Such testing would confirm that the different parts of the system work together correctly.

Appendix A – Referenced Documents

No.	Company	Title	Date
1	DoEHLG	*Security and Audit Features of the Election Management System*	Jan 2004
2		*Response by successful tenderer to Questions in RFT section 4 appendix F*	
3		*Electronic Voting and Counting System Information Paper*	Jan 2004
4	ERS	*Software Validation Report*	15-12-2003
5	KEMA	*Certificate No. 2028725.01 issued to NEDAP*	20-06-2003
6	Nathean	*Architectural Assessment and Code Review of IES for use at June 2004 Elections*	23-12-2003
7		*Code Review of IES Build 0111*	23-12-2003
8	Nedap	*Functional Specification – Nedap Voting System ESI2*	11-04-2003
9	Policy Institute TCD	*Proposed Research by the Policy Institute, Trinity College Dublin, for Commission on Electronic Voting*	11-03-2004
10	PTB	*Test Report*	20-03-2003
11		*Test Report 2*	17-09-2003
12		*Software Requirements for Voting Machines*	18-03-2003
13		*Test Report*	08-09-1998
14	TNO	*Test Report: Program Reading Unit Model ESI 1*	28-10-2003

No.	**Company**	**Title**	**Date**
15		*Test Report: Voting Machine Type ESI 2 (Standards IEC 60839-1-2, etc)*	30-06-2003
16		*Test Report: Voting Machine Type ESI 2 (Standards IEC 60839-1-3)*	29-10-2003
17		*Test Report: Voting Machine Model PRU (Standards EN 50082-2, etc)*	06-08-2003
18		*Test Report: Voting Machine Model PRU (Standards IEC 60068-2, etc)*	08-08-2003
19	Zerflow	*Electronic Voting Security Assessment*	27-03-2002
20		*Review*	04-07-2003