Part 3

Technical Aspects and Testing of the Chosen System

3.1 Introduction (*Part 3*)

This part reports the Commission's work in reviewing technical aspects and testing of the hardware and software components of the chosen system. The overall approach to this work was described in *section 2.3* of *Part 2*.

Each main hardware and software component of the system and its use is described individually in *section 3.2* (hardware) and *section 3.3* (software) of this part, together with a report of the desk reviews, analysis and testing of each component carried out by the Commission and the principal findings arising from this work in each case. *Section 3.4* provides an overview of the testing work carried out across all components. The Commission's conclusion on technical aspects and testing is set out in *section 3.5*.

The general features and proposed use of each main component of the chosen system are described in this part, either as they are intended and described by the Manufacturers or the Department, or as they have been observed by the Commission in the course of its work. However, in the detailed work that underlies this report, any assumptions or other limitations concerning the Commission's consideration of the system have been clearly identified and, where necessary or appropriate, these are stated in summarising the work below.

Some of the information received from the Manufacturers or otherwise obtained by the Commission in the course of its work is confidential or may relate to the security of elections. The Commission has refrained from including such information in the following descriptions of the system, and in reporting on its work and findings generally, but this information has been taken into account in arriving at the Commission's conclusion on technical aspects of the system in this part. For this reason also, the Commission has refrained from publishing the full details of the work carried out in its original form.

As indicated in *Part 2*, the purpose of the work carried out by the Commission in relation to technical aspects and testing of the chosen system was primarily investigative in nature. In particular, the work was designed to gather sufficient evidence to enable the Commission to form a definitive opinion of the chosen system. Different techniques of analysis and different approaches to testing were adopted in different measures according to their relevance and suitability to meeting this requirement. The work was not intended to provide exhaustive proof regarding the integrity of the system (although many of the techniques and approaches described would be applicable) as this would be an exercise beyond the scope and timeframe of the Commission's current remit.

3.2 Review of Hardware Components

This section describes the general features and proposed use of each main hardware component of the chosen system, together with the desk review and testing of each component carried out by the Commission and the principal findings of that work.

Appendix 1 contains an overview and illustrations of the main components of the chosen system, together with a description of its proposed operation at elections in Ireland. *Appendix 3* contains a description of the technical features of the chosen system provided by the Manufacturers for the purposes of the Commission's work.

Particular attention is paid in this section to the voting machine as this is the component of the chosen system that has the greatest public visibility. Together with the ballot module, the voting machine is also critically involved in the processes of gathering and recording votes at elections. These processes, unlike the sorting and counting processes carried out subsequently by other components of the system, cannot be repeated or authenticated without holding a fresh election. Also, seen from the voters' perspective, important questions arise concerning their use of the voting machine, including whether the voting process is secret, whether their vote is recorded at all and whether it is recorded accurately.

3.2.1 The Voting Machine

(a) Description and Use of the Voting Machine

General Description

The voting machine is used by voters to record their votes at polling centres. It is a portable device, having the appearance of a large suitcase when not in use, which can be opened up and placed on a table of suitable height to form a polling booth. An operator's control unit is remotely attached to the voting machine by a length of cable. The voting machine is illustrated in *Appendix 1*.

Broadly speaking, each voting machine represents a single polling station (officials' desk and ballot box) located within a given polling centre (school hall, etc.). Under the current paper system, this is the location at which voters are identified from the electoral register and issued with ballot papers, and at which they later place their votes in the ballot box. Under electronic voting, the identification of voters from the register would continue to be done manually as at present, while the voting process would be quite different.

Under the chosen system as currently proposed, approximately 7,000 voting machines, including backup machines, would be deployed at a national election. Several hundred voters would typically record their votes on each machine. An appropriate number of voting machines has been issued to each of the 23 Dáil election returning officers across 42 Dáil constituencies who coordinate arrangements for polling at elections of all types, as well as at referenda. Between elections, the voting machines are retained locally by the returning officers in secure storage. The security of the arrangements for storing the electronic voting equipment is reviewed in *Part 4* of this report.

Each voting machine has a unique identification number (ID) recorded electronically within the machine and imprinted physically on a plate fixed to the machine's outer casing.

Preparation for Use at Elections

At election time, the voting machine is removed from storage, tested for functionality and prepared for use by election officials in the days immediately before the poll. A programmed ballot module (see *section 3.2.2* below) is inserted, locked and sealed in position under a plastic cover at the rear of the machine and one or more replica ballot papers is inserted and locked under a clear transparent membrane on the voter's panel at the front of the machine.

The replica ballot paper is identical in appearance to those used under the paper system of voting save that each of the boxes in which the voter would mark their preferences contains an image of a button. The replica ballot paper is printed, and is aligned within a column on the voter's panel of the voting machine, so that each button image lies on top of a real button and opposite an LED numeric display on the voter's panel. There is room for up to five such ballot papers, to be used when more than one election or referendum is held at the same time.

The voting machine is switched on and the correct correlation between the electronic assignment of candidates and candidate details to buttons on the voting machine; the corresponding information on each replica ballot paper is tested before the machine is closed and sealed, ready for use on polling day.

Use of Voting Machine by Voters

From the perspective of the voter, the process of voting commences under electronic voting in the same way as it does under paper voting. Voters present themselves at the appropriate desk (polling station) within a polling centre in the usual way and are authorised to vote with reference to the electoral register. Instead of receiving ballot papers, however, they are issued with a voting slip indicating the polls they are entitled to vote in. The voter then presents this voting slip to the operator of an adjacent voting machine who presses a button on a control unit (described below) to activate for use by the voter only those ballot paper columns on the voting machine which correspond to the voter's entitlements as recorded on the voting slip.

The voter then uses the voting machine to record his/her preferences and finally casts a vote:

- For each poll in which they are entitled to cast a vote, the voter expresses preferences by pressing the buttons on the appropriate ballot paper in the sequence of their preferred choices. Thus the first button pressed expresses a first preference, the second button pressed a second preference, and so on. As each button is pressed, the corresponding preference number is displayed on the LED display beside that button. If an error is made, and is noticed by the voter, pressing any button a second time causes that preference and all lower preferences to be deleted. The sequence can be deleted or revised repeatedly in this way until the voter is satisfied with the selection to be recorded. As each preference is selected, detailed information about that preference is displayed on a small LCD display at the top of the voter's panel and an audible beep is sounded.

- This process is repeated for each ballot paper in relation to which the voter is entitled to cast a vote.

- The voter's LCD display at the top of the voter's panel is used to display preference details (candidate name, party, etc.) and other information regarding the use of the machine during voting. This information can be displayed in either the Irish or English language, chosen by the voter using a button located at the top of the voter's panel.

- After selecting preferences on the various ballot papers, the voter casts their votes on all ballots at the same time by pressing a "cast vote" button located at the top of the voter's panel. An audible beep, accompanied by a message displayed on the voter's LCD display confirms that the vote has been cast. The voter's panel is then automatically cleared and is no longer available for use by the voter.

- If preferences have been recorded on one or more, but not all, ballots when the "cast vote" button is pressed, a warning message is displayed on the voter's LCD display, accompanied by an audible beep, the vote is not cast and the voting machine remains activated for voting. In this case the voter may either confirm his or her intentions by pressing the "cast vote" button again (in which case only ballots with preferences selected are cast as votes[22]) or else the voter may return to express preferences on the remaining ballots before casting all their ballots together.

- If no preference has been expressed on any ballot when the "cast vote" button is pressed, no warning message is displayed on the voter's LCD display, no audible beep is heard and the voting machine remains activated for voting.

Following the initial activation of the voting machine by the operator for use by a voter, the voter is not required to make any further contact with the operator and may leave the machine at any time before, during or after voting, or indeed without voting at all. If the operator observes that the machine is unattended by a voter but remains activated for voting (as indicated by an LCD display on the operator's control unit – see below), they must deactivate the machine via a key switch on the control unit before activating it for use by another voter. This clears the voter's panel of any preferences that may have been selected and no vote is recorded[23].

Voting Machine Control Unit

The control unit is connected by a cable to the voting machine and consists of two sets of buttons, a key switch and an LCD display. One set of buttons is used during the poll to select the entitlements appropriate to each voter (as indicated by the voter's voting slip in each case) and the other set of buttons is used to administer the voting machine before and after the poll.

During administration of the voting machine before and after the poll, the key switch activates an alpha-numeric keypad hidden under a flap at the top of the voter's panel of the voting machine and

[22] When the voting machine records a vote in respect of a voter who has selected preferences in some but not all ballots, those ballots on which no preferences are selected are, in fact, also recorded as empty votes within the voting machine and are accounted for as "null votes". However these "null votes" are not counted under Irish election rules and must be deducted from the total number of votes recorded by the voting machine.

[23] The number of deactivations of the voting machine by the operator in circumstances where a voter has left the voting machine without pressing the "cast vote" button is also recorded by the voting machine.

intended for use by the operator only. During administration of the voting machine, operator information is displayed on the LCD displays located on both the operator's control unit and the voter's panel of the voting machine.

During polling, the operator uses the key switch to activate the voting machine prior to its first use and to deactivate and reactivate it as necessary if a voter does not cast a vote. The LCD display on the control unit displays (to the operator only) the status of the voting machine during polling and the total number of votes cast on it, while the LCD display on the voter's panel displays (to the voter only) only vote preference information and other messages regarding the voting procedure. However, certain error messages regarding incorrect use or functioning of the voting machine during polling are also displayed on the LCD displays located on both the control unit and the voting machine.

At the open and close of the poll, the operator causes the voting machine to print out a status report from a small printer located at the back of the voting machine. This printout includes the description and date of the poll(s), candidate information and their assignment to button locations, the Irish and English language messages for voters, messages for the operator, the number of votes (including null votes) contained in the ballot module, the number of activations and deactivations of the voting machine, the ballot module and voting machine identification numbers, check-sums and the software and hardware version numbers for the voting machine in question.

Following the printing of the status report at the close of poll, the votes and other poll data contained on the ballot module within the voting machine are then copied to a backup module within the voting machine before the main ballot module is removed from the voting machine.

(b) Desk Review of the Voting Machine

The security of the voting machine hardware was investigated by identification and examination of its components and sub-components and by reference to system documentation and other information provided by domain experts, including the Manufacturers and election personnel with knowledge and experience of previous use of the system for elections in Ireland. The focus of this investigation was on properties and behaviour of the voting machine that could affect the secrecy or accuracy of an election.

Particular attention was paid to the communications and information flows involving the sub-components of the external voter's panel screen[24], the internal voting machine module[25], the remote operator's control unit[26] and the printer[27]. In particular, information flows between the voter's panel screen and the voting machine module relate specifically to the "mapping" of physical external voter preference buttons to the candidate and other preference details for each poll actually recorded

[24] The voter's panel screen includes the external preference buttons, the "cast vote" button, the LCD/LED displays used by the voter, the Irish/English language button, the operator's keypad and 5 internal display boards each connected to a column of external preference buttons and LED displays. A connection board communicates between the display boards and the voting machine module (see below).
[25] The voting machine module includes a microprocessor and removable primary and backup ballot modules inserted in reading/writing slots accessible by the operator at the back of the voting machine.
[26] The control unit includes voter entitlement selection buttons, function buttons, a key switch and an LCD display and is connected to the voting machine module by a length of cable.
[27] The printer is a small thermal printer located within the voting machine and connected to the voting machine module.

electronically within the voting machine. This is the crucial part of the system that ensures the voter's expressed intentions are in fact secretly and accurately recorded on the ballot module.

Device Model

The voting machine was first modelled as part of a wider model of the chosen system as a whole. Additionally, the operation modes of the voting machine were modelled as a state diagram. Using the model and the state diagram, communications and information flows between the components of the voting machine at stages before, during and after polling were identified. The polling stage was then selected for closer examination.

Vulnerability Analysis

A vulnerability analysis of the polling stage was performed using a HAZOP[28] technique to explore what possible failures could occur in each component of the voting machine, whether they are detected or corrected by design features, and if they could propagate to cause undesirable outcomes.

A fault tree analysis[29] technique was then applied to selected potential vulnerabilities identified from the HAZOP analysis, in particular the possible inaccurate recording of a vote. The analysis traced backwards from this undesirable outcome to identify the events that would need to occur for it to happen, thereby identifying how the voting machine might be vulnerable to either malicious interference or incorrect operation.

Finally, an analysis of the information flows into and out of the voting machine was conducted to identify potential routes by which voter secrecy might be breached via the various input and output channels including LCD and LED displays, primary and backup ballot modules, volatile and non-volatile internal memory, keypad, preference buttons, control unit buttons and "cast vote" buttons, power supply, light, audio and radiated electromagnetic emissions. Selected channels were then considered in the context of access by the operator, the voter or others present during voting, and in the context of people who may subsequently have access to any permanently recorded output of vote data.

The presence within the voting machine of a data channel designed to assist visually impaired voters (but not used for the Irish application of the machine) was identified subsequently arising from the analysis of the embedded C code software component of the system described in *section 3.3.1*. This channel was also included in the analysis of potential hardware vulnerabilities.

During the above analyses, detailed questions relating to the design and intended behaviour of the voting machine were raised with the Manufacturers, and responded to by them.

Where properties and behaviour of the voting machine hardware were found to be reliant on the behaviour of its software components, these were highlighted as requiring separate investigation

[28] HAZOP (HAZard and OPerability) analysis is a method of identifying vulnerabilities within system processes. It involves a brainstorming approach that brings together system specialists to develop and analyse scenarios which could lead to safety failures. HAZOP is defined in UK Defence Standard 00-58.

[29] Fault Tree Analysis (FTA) is a qualitative analysis method that can be used to postulate in a top-down manner the likely events that would need to occur within a process in order to give rise to known outcomes.

and some of these were taken up as inputs to the investigation of the embedded C code software of the voting machine in *section 3.3.1*.

The analysis work described above, together with analyses of other components of the chosen system, provided the Commission with a detailed functional view of the voting machine, both from the inside out and as a component within the system as a whole. Potential vulnerabilities of the voting machine identified in the course of this review as having a bearing on secrecy or accuracy were reviewed by the Commission and, where appropriate having regard to security and confidentiality considerations, these vulnerabilities are reflected in the Commission's findings, listed further below. It should be noted that these potential vulnerabilities have not generally been assessed or ranked by the Commission according to their likelihood of occurrence at this time. They have, however, been considered in the context of vulnerabilities that have emerged from the Commission's work in relation to other aspects of the chosen system, including software and physical security aspects.

Usability Analysis

The Commission observed in its first report[30] that, notwithstanding some criticisms of the usability of the voting machine, it was easily understood in both concept and practical use and that, from the voter's point of view, its booth design and replica ballot paper interface maintain a helpful linkage to the existing paper voting procedure. While comparisons with other systems are beyond the scope of the Commission's work in relation to the chosen system, it is worth noting that not all electronic voting systems appear to offer voters the same compatibility with familiar paper systems.

Some further usability issues which may affect the secrecy or accuracy of an election have arisen in the course of the Commission's further work. These are in addition to the concerns cited previously by the Commission, which included issues of accessibility and secrecy for disabled persons and for those who are unfamiliar with, or fear, technology.

(c) Testing of the Voting Machine

Previous tests of the voting machine carried out by the Commission related mainly to investigating its accuracy in gathering and recording votes. In particular, the input-output volume test described below simulated an election in which large numbers of pre-determined votes were cast and counted and the results checked against the expected outcome.

While this type of "black box" testing demonstrated that the voting machine can accurately record voter preferences on the basis of known inputs and expected outputs, the Commission determined that sufficient proof of the reliability with which it does so, including as regards secrecy aspects, could only be obtained from analysis of the C code software embedded within the voting machine. Consequently, the Commission also undertook work in relation to the embedded C code software of the voting machine as described in *section 3.3.1*.

The Commission's further testing of the voting machine for the purposes of this section accordingly concentrated on its secrecy and accuracy properties from a hardware only perspective.

[30] First Report of the Commission on Electronic Voting, December, 2004: Part 4 p.55.

Electromagnetic Susceptibility and Compliance[31]

The voting machine was submitted to tests designed to investigate its susceptibility to electromagnetic eavesdropping and interference.

Electromagnetic eavesdropping involves the use of electronic surveillance devices to intercept electromagnetic radiation emitted by an electronic voting device while it is in use. If it is possible to interpret these signals and to associate them with an observed sequence of voters using the machine, then the eavesdropper can potentially breach the secrecy of the ballot.

Electromagnetic interference involves the disruption of the components and data of an electronic voting device while it is in use, by electrostatic discharge or radio frequency signals. Such disruption, which may be intentional or unintentional, could cause votes to become corrupted before or after storage, or not to be stored at all, and could potentially affect the accuracy of an election.

The likelihood of such occurrences on a widespread scale is considered small, given the degree of difficulty in gaining either covert or extended access to a significant number of electronic voting devices during an election and given also the range-dependent nature of the specialised surveillance equipment required, the effort required to interpret any data intercepted by eavesdropping and the highly localised nature of the disruptive interference effect. Any potential susceptibility of the components of the chosen system to electromagnetic eavesdropping and disruption is thus more of a threat to public confidence in the chosen system than it is a substantive systematic threat to the system's secrecy or accuracy.

Standards: Prior to the carrying out of the electromagnetic performance tests described below, the reports and other documentary evidence of previous certification testing of the device were reviewed, both to establish its levels of compliance with recognised standards and to evaluate the appropriateness of the standards applied. Although several countries have developed standards to meet their own testing and certification needs in introducing electronic voting, there is currently no internationally agreed standard for the electromagnetic compliance testing of electronic voting equipment. While the threats to such equipment are not currently well defined, a number of existing standards are nonetheless appropriate and applicable in the context of the public environment in which such equipment may be used at elections. The Commission's testing of the system was designed to meet or exceed these standards.

Guidance to users of the machine: It was also noted that the system manuals and official guidelines for deployment and use of the voting machine contain no information about its electromagnetic performance and offer no specific guidance on the need to locate the equipment away from potential sources of intentional or unintentional electromagnetic interference.

Construction: The construction of the device was examined to establish the methods of filtering and shielding and other design measures that had been implemented to limit its susceptibility to electromagnetic surveillance and interference.

[31] The review of electromagnetic susceptibility and compliance (EMC) standards, performance and other activities and tests described here in the specific context of the voting machine were also applied to the ballot module, the programming/reading unit and the hardened PC. Hence the object under review is described generically as "the device" in each case to facilitate subsequent reference to the activities and tests in the context of these components also.

Vulnerability: The internal components of the device were considered in light of their known or likely electromagnetic properties and in the context of their specific functions at significant stages of the voting process. A matrix of potential vulnerabilities of the device was then drawn up and prioritised to inform the test programme.

Surveillance Tests: The device was placed in an operational state and tested to determine if its electromagnetic outputs could be detected by a receiver and whether any such outputs could be correlated with functions carried out by the device when it was exercised normally during testing.

Interference Tests[32]: The device was also tested in an operational state to determine if its functioning was affected by radio frequency (RF) disruption and electrostatic discharges (ESD). However, due to the severity of some of these tests, it was not possible for test personnel to be in close proximity so as to fully exercise all normal functions of the device. Further testing via a suitably constructed remote control robotic arm would thus be required to confirm these functions.

Power Supply Tests[33]: Finally, the device's susceptibility to voltage dips and interrupts of the mains power supply was tested at selected appropriate points during its operation.

Volume Testing

A previous input-output volume test of the voting machine described in the Commission's first report[34] tested a significant sample of 739 voting machines assigned to returning officers throughout the country. These were used by the Commission to input 36,950 pre-determined votes and the tests confirmed that the machines had correctly recorded those votes. As the same version of the voting machine was provided to the Commission for the purposes of this report, it was not necessary to repeat this particular test.

It proved more difficult than anticipated, however, for the Commission to extend its volume testing of the voting machine to a much more rigorous level. Although this is not evident in ordinary use by a single voter, the voting machine's user interface proved to be both a slow and an unwieldy way to enter large numbers of votes accurately in the input-output test referred to above. In order to carry out more taxing tests of the system, involving very large numbers of pre-determined votes the Commission sought to bypass the user interface of the voting machine. If the user interface could be bypassed while still retaining the vote storage procedure and other significant functions of the voting machine, very large databases of known votes that would thoroughly tax the capabilities of the whole system could be entered in a reliable manner and with far greater speed and accuracy than permitted by the user interface. However it did not prove feasible, notwithstanding the cooperation of the Manufacturers, to procure a suitable test harness that would automate the entry of known vote databases into the system and thereby enable more thorough end-to-end testing of the entire system, not simply the voting machine. This inability to automate the entry of large vote databases also had a significant impact on the Commission's ability to tax the capabilities of other components of the system further "downstream" from the voting machine in a substantive and authentic manner.

[32] Electrostatic Discharge Tests: BS EN 61000-4-2: 1995 "Testing and Measurement Techniques – Electrostatic Discharge Immunity Test".
[33] Voltage Dips and Interrupts Tests: BS EN 61000-2-4: 2002, "Electromagnetic Compatibility (EMC) – Part 2-4 Environment Compatibility Levels in Industrial Plants for Low Frequency Conducted Disturbances".
[34] First Report of the Commission on Electronic Voting, December, 2004: Part 2 p.32; Appendix 2C p.167.

The Commission's conclusions on input-output volume testing of the voting machine are thus based on the results of the "black box" testing presented in its first report.

(d) Principal Findings Concerning the Voting Machine

This section sets out the main findings emerging from the Commission's desk review and testing of the operation of the voting machine, from the perspective of the secrecy and accuracy of the ballot.

Vulnerability Analysis

While design features have been incorporated to protect against some hardware failures, the Commission's work, described above, has shown that protection against other potential vulnerabilities of the voting machine relies variously on the following to detect and report failure, error or other incorrect behaviour of the voting machine:

- the voter and/or voting machine operator;
- the hardware itself;
- the embedded software.

These issues are discussed in the following paragraphs.

Reliance on Voters and/or Operators to Detect Faults

The vast majority of voters must vote alone and unaided. Voters will have a wide range of ages, abilities and levels of technical competence. All voters will be unfamiliar with the voting machine, at least during the first elections in which it is used. It is quite likely, furthermore, that voters will not detect actual failures of the voting machine that may occur during polling and this is something that cannot be easily mitigated by voter education policies. Any system of electronic voting must therefore be designed in a way that does not compromise the secrecy and accuracy with which the views of even the least able voters are recorded.

The Commission's work has indicated that there is some reliance on voters and operators to observe any possible failure or incorrect behaviour of the voting machine while it is in use at polling centres on polling day. However, failures arising from the use of the voting machine by an authorised operator, before, during or after the poll are of lesser concern than those which arise during use by voters, assuming that a high level of training and guidance information on the use of the system will have been provided, enabling operators to detect such occurrences as effectively as possible.

Hardware Vulnerabilities: Electromagnetic Eavesdropping and Interference

The Commission's testing of electromagnetic performance indicated no major malfunction or susceptibility of the device[35] to threats of interference, disruption or eavesdropping. Test results

[35] The findings regarding electromagnetic susceptibility and compliance (EMC) standards and other activities and tests described here in the specific context of the voting machine are also applicable to the programming/reading unit and the ballot module (but not the hardened PC). Hence the object under review is described generically as "the device" in each case to facilitate subsequent reference in the context of these components also.

obtained thus far indicate the following:

- previous compliance tests of the device were inadequate to confirm its electromagnetic performance for the purpose of its use in the context of public elections;

- more rigorous tests carried out by the Commission have nonetheless established that the device is robust against significant electromagnetic threats of interference or eavesdropping;

- further electromagnetic performance testing of the device while its critical functions are being exercised would be desirable.

In the course of these tests, it was observed that no specific operator guidance is given on how to locate electronic voting hardware so as to minimise its susceptibility to electromagnetic threats at elections, whether intended or unintended.

In addition, it was suggested that, as there is currently no specific internationally agreed standard in respect of electronic voting equipment, the information gathered in the course of preparing and carrying out these electromagnetic compliance tests could make a valuable contribution to the development of proposed international standards that are currently under consideration[36].

Other Hardware Vulnerabilities

While successful remote electromagnetic eavesdropping or interference seem very unlikely, the Commission's work has also revealed other vulnerabilities that could potentially arise once an unauthorised person with technical knowledge has direct physical access to a voting machine.

In this regard, a specific albeit very remote vulnerability has been identified by the Commission, involving the possible alteration of the software mapping from external voter preference selection buttons to corresponding electronic registers within the voting machine, causing an incorrect vote to be stored. The likelihood of occurrence of this vulnerability is considered remote on the basis that it would require a determined hacker with specialist knowledge and hardware and software tools. The impact of such an attack in terms of affecting the outcome of an election is low as it would be necessary to gain access to a number of voting machines for a considerable period of time. Such an attack would nonetheless be worrying since it would be very difficult to detect while, if detected, it would have a serious impact on public confidence in the entire system of elections.

The Commission's analysis has also indicated a potential vulnerability that may arise from a feature of the system designed to facilitate voting by visually impaired persons via a physical external data link, which remains present but unused within the voting machine in its Irish application. Taken with the presence also of the corresponding embedded C code software within the voting machine to control this data link, there is uncertainty as to the degree to which the functioning of this feature has been fully deactivated for its intended, or possibly unintended, use. This data link from the voting machine to the external world thus represents a further potential vulnerability of the machine to malicious and technically skilled attacks, particularly those targeted at breaching the secrecy of the ballot.

[36] IEEE P1642/3 "Recommended Practice for Protecting a) Public Accessible Computer Systems and b) Voting Systems and Equipment, from Intentional EMI" (due for completion December 2007).
IEEE P1583 "Voting Equipment Standard" Committee established 20 October 2003.

As indicated in the Manufacturers' technical description of the system in *Appendix 3*, the voting machine contains the same main electronics board and embedded C code software as the programming/reading unit (see *section 3.2.3* below). It is further understood from the Commission's work that the voting machine and the programming/reading unit are conceived as essentially the same device, with appropriate interventions and additions being made to its hardware and software configuration during manufacture to determine whether a particular unit will become a voting machine or a programming/reading unit. Arising from this, it may be possible, given the relevant knowledge and tools, to adapt a voting machine into a programming/reading unit. If so, this has the implication that an attacker with access to a single voting machine and the appropriate technical knowledge could adapt it to become a programming/reading unit that could be used to program ballot modules. This in turn reinforces the attention that must be paid to arrangements for the secure storage of voting machines, as well as programming/reading units. These arrangements are reviewed in *Part 4* of this report.

In reality, these potential hardware vulnerabilities of the voting machine present only a very remote threat to the accuracy or secrecy of elections as they depend upon specific knowledge, tools and direct physical access to voting equipment by unauthorised persons. However, when considered together, they draw particular attention to the need to consider access controls and other physical security arrangements for the storage, management and use of voting machines and other equipment in order to ensure confidence in the security of the system. Physical security aspects of the voting machine are thus central to the security of the chosen system as a whole and they are reviewed in *Part 4*.

Reliance on Embedded Software

In considering the behaviour of the voting machine hardware from the perspectives of secrecy and accuracy, it has been assumed that its embedded C code software operates exactly as expected. Indeed the assumed or intended operation of this software has been cited by the Manufacturers as providing protection against particular hardware vulnerabilities. There is thus a significant reliance within the chosen system on the behaviour of the embedded software of the voting machine.

This indicates that all relevant code of the voting machine software should be carefully investigated to establish whether, and how, it protects against the potential vulnerabilities noted above, as well as those noted elsewhere in this report in respect of the other components of the system. Careful investigation is further warranted because any vulnerability or undesirable behaviour inherent in the software's design (rather than being maliciously introduced into one or more individual machines) will be present in every voting machine in which the software is installed, causing a potential for system-wide problems.

The Commission has not conducted a line-by-line review of the software embedded in the voting machine. However, the Commission's analysis of information flows through the various input and output channels of the voting machine hardware indicates that it is necessary to investigate and confirm the functioning of the embedded C code software in order to assure voters that their vote is secret in the following respects:

- no voter preference information should be capable of being passed to the printer, the control unit LCD, the sound synthesiser or any other input or output device including, in particular, the unused voting facility for the visually impaired identified by the Commission;

- it should not be possible to recover any preference information from the voter's LED display, the voter's or operator's LCD displays or any other input or output device, including the unused voting facility for the visually impaired, once the voter has cast their vote;

- it should not be possible to recover any preference information from the non-volatile memory of the voting machine that is used to store a vote in the case of power failure.

It would also be important to confirm in further analysis that the election configuration data that is read by the voting machine from the ballot module at the opening of the poll is checked subsequently, and with sufficient frequency, by the voting machine software against the ballot module to ensure that it remains consistent with its original state at all times during polling. This is necessary to ensure that the assignment of candidates to preference buttons on the voter interface does not become altered during voting as a result of malicious interference in such a way that, while the machine appears to be operating correctly, votes are in fact being assigned to candidates other than those intended by the voter.

Software and Hardware Security: Access Controls and Authentication

Although measures such as key switches, locks, tamper detection seals and other physical security features have been applied to the voting machine as described above, no additional security measures such as password or other code protections have been implemented within the software and hardware of the voting machine by which operators or voters must identify themselves before they gain access to its ordinary services while in use before, during and after polling. Such measures are now commonplace in electronic systems deployed for use in a public setting.

Additionally, in cases where there is an observed failure or other incorrect behaviour of the voting machine, the operator is required to note any error code displayed by the voting machine and to contact a help desk provided by the Manufacturers. Problems are then diagnosed remotely and, where possible, addressed by the operator with remote assistance from a qualified engineer. In cases where a problem with the voting machine cannot be addressed in this way, the voting machine must be sent to the Manufacturers for further analysis. Similar arrangements apply in respect of ballot modules and programming/reading units. It would thus appear that higher levels of access to core services of the voting machine and other equipment deployed within the chosen system are afforded to system engineers than to election officials at any stage.

The Commission has observed no mechanism within the system that would enable operators, observers and voters to satisfy themselves independently that the hardware and software of the voting machine are authentic and that they are the correct versions that have been tested and certified and that have been approved for use by the electoral authorities. The system is essentially self-checking in this respect.

Usability: Ballots that do not Reflect the Intentions of the Voter (Accuracy)

The Commission's usability analysis has highlighted scenarios in which, even though the system is working correctly, voters may not realise – or may not realise in time – that the system is not recording votes in the way they expect it to. In particular, the user interface of the voting machine may cause voters to cast their ballots in an unintentional manner, thus affecting the accuracy of the

ballot, in the following ways:

- The method by which every ballot must be fully completed before all ballots can be cast together may not seem natural to some voters. Thus, when multiple polls are conducted simultaneously, there may be voters who, having selected their preferences in one poll will seek to cast their ballot for that poll before proceeding to select preferences for the next ballot. Note that, under paper voting, ballots can be completed and cast individually if the voter so wishes.

- There is also an inconsistency of the voting machine's behaviour already noted in the Commission's first report[37] whereby it is possible, in the case of the ballots at simultaneous polls, to exercise the "cast vote" button when no preferences are selected on some, but not all, of the ballots while, in the ballot at a single poll, it is not possible to exercise the "cast vote" button when no preference has been selected. The related issue of how the chosen system handles null or blank votes is discussed in *Appendix 5A*.

- There may also be voters who try to record each individual preference within a ballot separately by pressing the "cast vote" button immediately after they have selected that preference. This could be a particular problem when only a single election was being held. If a voter tries to record each preference individually in the ballot for a single poll by pressing the "cast vote" button, their vote will be recorded as containing their first preference only, the voter's display will be cleared and it will not then be possible for them to express further preferences.

- While the above examples describe the correct and intended behaviour of the voting machine, they draw attention to a further inconsistency in the interaction between voting machine and voter. Whereas an error message is used to alert voters that they are about to take a possibly unintended action (i.e. by expressing preferences in some but not other ballots at multiple polls), no equivalent message is displayed, in cases when there is a single ballot on the machine, inviting voters, before they cast any vote, to confirm the action they are about to take is that which they intend.

  Such confirmation messages are now commonplace in automated electronic systems for public use and users of such systems expect to be asked by the machine to confirm their indicated action as their intended one. It seems very desirable that users of electronic voting machines should also be given an opportunity, by whatever means, to confirm their intended actions as well as being warned of possibly unintended actions before being committed to these.

- In those circumstances where a warning message is displayed, the message appears on the LCD display at the top of the voter's panel, flashing three times, and a beep will sound drawing the voter's attention to the fact that there is at least one ballot with no preference indicated. However the LCD display is relatively small and is not closely integrated with the preference selection interface. The message may thus either remain unnoticed or be not easily visible by some voters, some of whom may press the "cast vote" button again, thus causing their vote to be cast unintentionally.

Although voter information policies can go some way to mitigating any possibility of precipitate or unintentional voting such as may arise in these circumstances, it would be preferable if these issues were addressed through careful review and modification of the behaviour of the voting machine

[37] First Report of the Commission on Electronic Voting, December, 2004: Part 3 p.46.

hardware and software so as to avoid such circumstances.

Usability: Inferring Voter Behaviour from Voting Machine (Secrecy)

While a number of minor criticisms concerning the "beeps" emitted by the voting machine were highlighted by the Commission's previous reports, no significant secrecy issues have arisen from the Commission's further work concerning the use of the voting machine by voters.

One such issue concerns the fact that the "cast vote" button is in close proximity to the preference buttons and LED displays and that this may facilitate voluntary or involuntary breaches of secrecy by way of video recording of the "cast vote" button being pressed while the voter's selected preferences are displayed. The technology to achieve this is now widely and cheaply available in the form of video phones and other compact and portable devices. However, the same technology would also facilitate similar breaches of secrecy under paper voting.

Accessibility and secrecy issues noted previously by the Commission[38] in relation to use of the voting machine by disabled persons, assisted voters and other persons who fear or are unfamiliar with technology continue to be relevant. However, the Commission has noted that the voting machine also provides enhanced accessibility to voting for other people in these categories (including those with literacy difficulties).

Usability: General

With the exception of the usability issue concerning the co-location of the "cast vote" button and LED preference displays, and the issue concerning the size and location of the LCD message display, all of the usability concerns in relation to secrecy and accuracy of the voting machine identified by the Commission are capable of being addressed by amendment of the embedded C code software or by minor modifications to the design of the voting machine hardware.

Volume Testing

It was not possible to bypass the voting machine's user interface for the purpose of taxing the voting machine and other "downstream" components of the system with very large numbers of known votes in the manner sought by the Commission. Although acting as a significant limitation on the Commission's proposed testing and research, this limitation is also a strength of the machine itself as it shows that there is a degree of difficulty presented to those, even with high technical ability and physical access, who seek to input votes to the machine by bypassing its interface. However, it is also important to note that this would not be the only way to introduce votes into the system as a whole, as the Commission's work in relation to other components of the system has indicated further below.

[38] First Report of the Commission on Electronic Voting, December, 2004: Part 5 p.67.

3.2.2 THE BALLOT MODULE

(a) Description and Use of the Ballot Module

General Description

The ballot module is a portable, reusable data storage device used before the poll to record, store and transport election data between election offices and polling centres and used after the poll to transport election data, including votes, between polling centres and count centres[39].

Approximately the size of an audio cassette box, the function of the ballot module under electronic voting corresponds closely to that of the ballot box under paper voting. It is used to store the votes cast at polling centres and to transport them to count centres. Votes are then extracted from the ballot module, associated with votes from other ballot modules pertaining to the same poll or polls, and mixed prior to counting.

However, the ballot module has an additional function that is not shared with the traditional ballot box. It is also programmed before the poll to contain the election data or "parameters" with which the voting machine is configured for use on polling day. The equivalent of this function under paper voting is the one or more sealed ballot boxes used by each presiding officer to store and transport books of ballot papers and other sensitive materials to the polling centre on polling day.

With the exception of the backup ballot modules (see below) which generally remain installed in voting machines, each ballot module has a unique identification number (ID) recorded electronically within it and imprinted on the outer casing.

When used at elections, the ballot module makes a two-way journey between the programming/reading unit (see *section 3.2.3* below) and the voting machine as described above.

Preparation for Use at Elections

In the days immediately before a poll, the ballot module is used as follows:

- The ballot module is first inserted into a "writing" slot on the programming/reading unit at the election office of the returning officer while the programming/reading unit is connected to a "security-hardened" PC (see *section 3.2.4* below) on which the election data has been set up using the election management software (see *section 3.3.2* below).

- The ballot module is then programmed with the election data or "parameters" for each poll including the date of poll, type of election, constituency, polling centre and polling station, candidates, candidate details and their intended assignment to physical preference buttons on the voting machine together with Irish and English language messages to voters, and other settings of the voting machine.

[39] The compact disc (CD) is also used in the transport of election data and votes before and after the poll – see *section 3.2.5* below.

- One ballot module is programmed[40] for each voting machine that will be used at the election, together with a number of spare ballot modules that may be used in any voting machine within a given electoral area if required in the event of failure of a ballot module or a voting machine on polling day.

- The ballot module is then removed from the programming/reading unit slot and it is inserted, locked and sealed in a similar slot within a voting machine which has previously been removed from storage and tested for functionality. Replica ballot papers containing the same election data as the ballot module are prepared separately using the election management software and are enclosed within the voting machine which is then configuration tested, closed and sealed.

- When the voting machine is switched on during testing, the election data or "parameters" from the ballot module are read by the voting machine and used to configure the voting machine for use, associating candidate details with the buttons and LED displays corresponding to the locations of those details on the replica ballot papers on the voter's panel.

The voting machines containing the programmed ballot modules are then ready for use by voters. They are stored until they are transported for use as polling stations within polling centres as described in *section 3.2.1* above. Once "primed" for an election in this way, the physical security of the voting machine and its installed ballot module is obviously of crucial significance in relation to the secrecy and accuracy of the election; this matter is dealt with in *Part 4* of this report.

Use on Polling Day

On polling day, the ballot module is used as follows at polling centres:

- When the voting machine is set up as a polling booth and switched on, the correct assignment of candidates to preference buttons and their alignment with the appropriate ballot papers and ballot paper entries can be tested again by the operator before polling commences. This can also be confirmed by a printout from the voting machine which records relevant poll details and the number of votes recorded on the ballot module (which should be zero).

- During polling, each time the "cast vote" button is pressed by a voter, the preferences they have selected on the voting machine are stored within the ballot module. The procedure for storing a vote is described further below.

- When the poll is closed by the operator, this causes a backup copy of the data on the ballot module to be recorded on another ballot module that is retained within the voting machine. These modules are distinguished as the primary ballot module and the backup ballot module. A printout is made of the same poll details, etc., as were printed out at the opening of the poll,

[40] There is no express requirement within the hardware or software of the chosen system that a particular ballot module must be used in a particular voting machine. Although the election management software tracks which ballot modules (by ID number) have been programmed for a particular election and the voting machine tracks the last three ballot modules installed within it, the installation of a particular ballot module in a particular voting machine and the allocation of a particular voting machine to a particular polling station are entirely reliant on the administrative procedures governing the use of the system at elections.

including the numbers of votes stored and the numbers of activations and deactivations of the voting machine during the poll.

Following the close of poll, the ballot module is used as follows:

- The primary ballot module is removed from the voting machine and sealed in an envelope with the open and close of poll printouts from the voting machine and other covering documents for transmission by hand to the count centre or, in some cases, to a read-in centre. At the count or read-in centre, the contents of the ballot module are read in, together with the contents of other ballot modules, using the programming/reading unit connected to a "security-hardened" PC on which the election was set up using the election management software as referred to above. In this way, the votes recorded on all of the ballot modules for the constituency are copied into a database within the election management software.

- The backup ballot module remains in the voting machine and is only referred to in the event that there is a query regarding the primary ballot module. It is automatically erased by the voting machine immediately before it is next used to make a backup.

Use after Elections

The primary ballot module containing the original votes cast is retained for 6 months after the poll as required by law before its contents are erased using the programming/reading unit. The backup module on the voting machine is not erased at this time and stays in the voting machine until the next election for which the machine is used – it is then automatically erased immediately before its next use to create a backup. It is thus necessary to provide a reserve ballot module for use in each of approximately 7000 voting machines in the event that polling at a further election or referendum occurs within six months of the previous one. Approximately 21,000 ballot modules in total, including backup ballot modules and spares, have accordingly been provided and are stored locally by returning officers for this purpose.

Storage of a Vote

When the "cast vote" button is pressed by the voter during the poll, the preferences that have been selected by the voter and displayed on the LED displays of the voter's panel of the voting machine are stored twice in each of two memory locations in the primary ballot module, that is, four copies of the vote are made.

Each stored vote contains an identifier of the poll or polls to which it relates, together with details of the voter's preferences at each poll. The vote is delineated from other votes by a start marker and an end marker. Each element of the vote is also accompanied by a check-sum.

The storage location of a vote within each memory location of a ballot module is determined pseudo-randomly, using the timer of the voting machine as a seed in the case of the first vote to be stored. Thereafter each vote is stored either immediately before or immediately after the other votes that have already been stored, with the question of whether it is stored before or after also being determined pseudo-randomly. If, as further votes are stored, a vote cannot be stored before the other votes as determined by this method, then it is stored after them (and vice versa) until it is no longer

possible to add votes to the ballot module.

In the event that power is lost after the "cast vote" button is pressed but before the vote is recorded, details of the vote are stored in the non-volatile memory of the voting machine itself and are recovered and stored in the ballot module when power is restored. The question of whether a particular vote has been recorded in these circumstances is reliant on the operator observing whether or not the total number of votes displayed on the LCD display of the control unit has been incremented in respect of the voter in question following restoration of power to the voting machine.

A ballot module can store approximately 28,000 preferences (i.e. voter choices for individual candidates) and the capacity of the ballot module to store whole votes is thus approximately equivalent to 28,000 divided by the average number of preferences recorded by each voter across all polls being taken simultaneously.

When a vote is stored, a block of memory is allocated which corresponds to the total number of preferences recorded by the voter across all polls. As indicated above, voters must express a preference in at least one poll to have their vote recorded but a null vote is recorded within the ballot module in respect of polls at which they express no preferences. However, although null votes are recorded as such within the ballot module, they are not formally recognised or counted as such under Irish election rules and must be deducted from the total number of votes recorded before the votes are counted.

After a vote is stored, the counter of votes stored within the ballot module is incremented and is displayed on the operator's LCD display. This display distinguishes between the numbers of votes that have been cast at each poll being taken but it does not distinguish whether or not the votes that have been cast actually contain preferences (as described in relation to the use of the voting machine in *section 3.2.1* above). Votes containing no preferences that are recorded by the voting machine in this way are, however, distinguished as such in the totals of votes recorded on the printouts from the voting machine.

The number of deactivations of the machine by the operator in circumstances where they observe that a voter leaves the machine without pressing the "cast vote" button (whether or not they have expressed preferences) is also recorded within the ballot module and on the voting machine printouts but is not displayed on the operator's LCD display. Preferences that remain on the voter's display when the voting machine is deactivated in this way are not stored as votes.

The printouts from the voting machine described further above are used to confirm that there are no votes already stored on the ballot module when the poll opens and to confirm the number of votes that have been cast at each poll when the poll is closed. After the close of poll and the copying of the votes to the backup ballot module, no more votes can be stored on the primary ballot module using the voting machine.

(b) Desk Review of the Ballot Module

The security of the ballot module was investigated by analysis and examination of its physical components and data structures and by reference to system documentation and other information provided by the Manufacturers. The focus of the investigation was on properties of the ballot module that could affect the secrecy or accuracy of an election.

Device Model

The ballot module was firstly modelled as part of a wider model of the whole system. Additionally, a circuit diagram of a memory device within the ballot module was examined.

The ballot module comprises two EEPROM[41] memory devices, together with associated circuitry and components, within a blue outer casing and a multi-pin plug for connecting the ballot module to a voting machine or programming/reading unit.

Data Model

As mentioned above, each vote is stored twice within each of two EEPROMs within the ballot module. There is thus redundancy within the ballot module in the event of failure of an individual memory location or in the event of corruption of one or more records of a vote within the ballot module as a whole. Further redundancy exists in the provision of a backup copy of the entire ballot module within the voting machine, thus causing there to be eight copies in total of each vote. However, as this backup copy is created at the close of poll, it is only of value during subsequent stages of an election and not while the votes are being cast.

The data structure within each memory device of the ballot module includes the following:

- the data that can be printed out from the voting machine as described in *section 3.2.1*;
- vote data stored as described above and below in this section;
- a "module closed" flag and a record of the number of times the ballot module has been erased.

Check-sums[42] are applied to some of this information while hamming codes[43] are applied locally within the data structure of each individual vote.

Vote Storage Capacity

In the context of the proposed use of the system at elections in Ireland, information provided by the Manufacturers has indicated that the capacity of the ballot module is more than adequate to store the number of votes that could be cast on a voting machine at any multiple poll, having particular regard to the likely average number of voters per voting machine and the distribution of voting machines across electoral population centres. The possibility that a particular module would become "full up" during ordinary use in the course of an election is thus remote.

[41] Electrically Erasable Programmable Read-Only Memory.
[42] Check-sums are used to detect corruption in blocks of data. The values that make up the block are added together and the result is transmitted or stored as an additional data value at the end of the block.
[43] Hamming Codes are a more sophisticated method of error detection involving the addition of three check bits to every four data bits. These codes can detect all single-bit and two-bit errors and can correct any single-bit error.

Vulnerability Analysis

Having regard to the components and data structures of the ballot module identified from the system model and circuit diagrams as described above, the possible failures of a ballot module were then considered using a failure modes and effects analysis (FMEA)[44] technique to consider the impact, detection and mitigation of possible failures that may be caused by a range of data inputs or component states of a single EEPROM memory device within a ballot module.

During the above analyses, detailed questions relating to the design of the ballot module were raised with the Manufacturers, and responded to by them.

(c) Testing of the Ballot Module

As indicated in relation to the voting machine described above, many of the secrecy and accuracy issues concerning the storage of votes on the ballot module depend on the reliability of the embedded C code software within the voting machine. The correct functioning of this software cannot be confirmed by demonstration through "black box" testing alone and it would be necessary to analyse the source code for this purpose. The work carried out by the Commission in this regard is reported in *section 3.3.1* of this part.

The Commission's testing of the ballot module for the purposes of this section accordingly concentrated on the secrecy and accuracy properties of the ballot module from a hardware perspective only.

Data Security and Integrity

The process of reading data from a ballot module was monitored via the serial interface between the programming/reading unit and the hardened PC. The commands and data exchanged between the programming/reading unit and the PC were then studied.

Electromagnetic Susceptibility and Compliance

As the ballot module is unpowered while in transit, a number of the electromagnetic eavesdropping and interference tests[45] carried out in relation to other component devices of the chosen system were not directly applicable to it in isolation.

However, as the voting machine and programming/reading unit were tested while they contained a ballot module, the ballot module in its powered state was included within the scope of the tests of these devices as described in *section 3.2.1* above. The description and outcome of those tests are thus applicable to the ballot module also.

In the context of other possible malicious threats to the integrity of the ballot module that may arise

[44] Failure Mode and Effect Analysis: FMEA from Theory to Execution, D H Stamis, ISBN 0873895983, 2003.
[45] See description of electromagnetic susceptibility and compliance tests of voting machine in *section 3.2.1* above.

while it is unpowered during transportation, a test[46] carried out previously by the Commission also remains relevant. In this test, a ballot module containing data was exposed to a very strong electromagnetic source of 7 Tesla[47].

Volume Testing

A previous input-output volume test of the voting machine described in the Commission's first report[48] confirmed that 36,950 pre-determined votes cast on 739 voting machines were correctly recorded on the 739 ballot modules deployed for the purpose of that test.

As indicated already in relation to the further volume testing of the voting machine which the Commission sought to carry out, although the user interface of the voting machine had proved both slow and unwieldy for entering large numbers of votes accurately in previous tests, the Commission found that it was unable to bypass this user interface for the purpose of further volume testing of downstream components of the system, including the ballot module.

The Commission accordingly sought to explore means of entering large numbers of known votes authentically into the system at a point further downstream from the voting machine. Methods of recording votes directly onto the ballot module via a test harness designed to replicate the function of the voting machine in recording votes on the ballot module were considered. It was intended by this means to test the general features of the ballot module as well as testing a large number of ballot modules under different conditions. However it did not prove feasible, notwithstanding the cooperation of the Manufacturers, to procure a suitable test harness with which to achieve this. As further testing of the ballot module itself was not the only objective, this also had a significant impact on the Commission's ability to carry out testing of other components of the system further downstream from the ballot module in a substantive and authentic manner.

The Commission's conclusions on input-output volume testing of the ballot module are thus based on the results of the "black box" testing presented in its first report.

(d) Principal Findings Concerning the Ballot Module

This section sets out the main findings emerging from the Commission's review and testing of the operation of the ballot module from the perspective of the secrecy and accuracy of the ballot.

Data Integrity

Before the poll, the most critical failure of a ballot module that could occur would be a corruption of the data or "parameters" that determine the assignment of candidate details to voting machine button positions. While it is expected that this should be detected by operators before polling commences, the following questions also arise regarding the need to ensure the continued integrity of ballot module data during subsequent stages of the voting process:

[46] First Report of the Commission on Electronic Voting, December, 2004: Appendix 2D p.197.
[47] Equipment to produce a magnetic field of this strength is in no sense portable or widely available, requiring a large and very expensive installation.
[48] First Report of the Commission on Electronic Voting, December, 2004: Part 2 p.32; Appendix 2C p.167.

- Is the assignment of candidates to buttons on the voting machine re-checked for consistency against the ballot module during polling?

- If the assignment of candidates to buttons is re-checked against the ballot module for consistency, what checks are there that the ballot module itself remains correct?

Additionally, during polling, any data failures that may arise in the storage of votes and other data in the ballot module should automatically be detected as part of the process of reading back data to check it for consistency after it has been stored.

After the poll, the most critical failure of a ballot module that could occur would be a corruption of vote data. Significant in this regard is how the integrity of this data is protected and ensured. Clarification is needed as to whether, how, and at what stage in the process, the two copies of each vote stored within each memory device, combined with the two memory devices contained within each ballot module, are used together to detect and recover from possible data errors.

In order to avoid the possible, if unlikely, loss of all vote data stored on the ballot module due to malfunction of the devices that write to or read from it, the adequacy of the voting machine and/or programming/reading unit functions designed to detect and protect against this should be confirmed.

In view of the above concerns, the software functions that are responsible for recording data on the ballot module and for ensuring and checking its integrity thus need to be investigated very thoroughly.

Although additional data redundancy is provided by the backup ballot module that is retained within the voting machine after the poll, this backup is created only when the poll has closed. The value of this backup as an independent parallel record of the votes already stored in four locations within the primary ballot module would be enhanced considerably if the backup was updated after each vote is stored.

Data Security

Arising from the analysis of information flows through the various input and output channels of the voting machine, described above, it is also necessary to investigate and confirm the function of the embedded C code software of the voting machine in order to assure voters that their vote as stored in the ballot module is secret in the following respects:

- voter preference data and no other voter information should be stored on the ballot module during voting;

- there should be no mechanism for recording or displaying the location of a particular vote in the ballot module;

- it should not be possible to infer a voter’s identity from the location of their vote in the ballot module.

Arising from penetration testing of the hardened PC while connected to a programming/reading unit

attached to a ballot module containing data as described in *section 3.2.3* below, data stored on ballot modules was found to be accessible with moderate ease:

- data on ballot modules is not encrypted to prevent unauthorised reading; it is stored, and can be recovered as, clear text: the use of public/private key cryptography would protect the data from being read if it were intercepted;

- data on ballot modules is not cryptographically signed to prevent unauthorised alteration: the use of public/private key cryptography would protect against attempted access and against malicious or accidental alteration of data while stored on the ballot module.

The protocols for applying check-sums to the data stored on the ballot module were also easily discovered. As a result it was found to be possible to extract data from the ballot module in clear text and it was suggested from this work that, given sufficient time, it might also be possible to discover by similar means the data structures necessary to write data to a ballot module.

Although simple check-sums are applied to some of the data on the ballot module, confidence in the secrecy of the ballot would be greatly enhanced if the data was protected from unauthorised access and disclosure by the cryptographic methods mentioned above, which are standard ways of protecting any sensitive electronic information.

Storage of Votes

All of the matters described above in relation to the integrity of the actual method of recording of votes on the ballot module, including in circumstances where the power fails during this process, are central to the secrecy and accuracy of an election and depend crucially on the assumption that the C code embedded in the voting machine does in fact perform as specified and expected. This is why it is so important for this code to be thoroughly investigated.

Hardware Vulnerabilities

The findings already recorded in this report in relation to the electromagnetic compliance testing of other component devices[49] of the chosen system are also applicable to the ballot module. In particular, the ballot module appears robust against significant threats of electromagnetic interference or eavesdropping while it is in static operational mode but further testing is recommended to observe its performance while its critical functions, including vote storage, are being exercised under certain test conditions.

Following the exposure of a ballot module containing data to a very strong electromagnetic source of 7 Tesla in previous testing by the Commission, the contents of the module were found to be unaffected.

Variations in internal construction were observed between different ballot modules provided to the Commission. This could be significant in the context of any official type-approval of voting equipment for use in Ireland.

[49] See description and findings of electromagnetic susceptibility and compliance tests of voting machine in *section 3.2.1*.

Volume Testing

As indicated further above in relation to testing of the voting machine, the Commission was also unable to exercise the ballot module and other downstream components of the system using large numbers of known votes introduced authentically by using a test harness either to bypass the voting machine interface or to introduce them directly onto the ballot module itself. Although this was a limitation on the Commission's proposed work, it also represents a strength of the system as it shows that there is a degree of difficulty presented to anyone seeking maliciously to introduce large numbers of votes or other data to the system at an election by recording them directly onto a ballot module.

General

If appropriate administrative and physical security procedures are applied to prevent with certainty any unauthorised access to every ballot module, then other potential vulnerabilities of the ballot module represent only a very remote threat and are unlikely to affect the result of an election. The physical security aspects of the chosen system that are relevant in this regard are discussed in *Part 4* of this report.

However the possibility of unauthorised access can never in practice be ruled out completely, while its potential impact on public confidence in the chosen system would be significant. This requires that any such potential weakness must be placed beyond all doubt and that the system must be made inherently more secure, and less dependent on physical security measures, by the implementation of the cryptographic security measures described above. Such measures can be implemented in a way that is transparent to users and operators of voting equipment and that will not impact on its simplicity or ease of use.

3.2.3 THE PROGRAMMING/READING UNIT

(a) Description and Use of the Programming/Reading Unit

General Description

The programming/reading unit is used by election officials both before and after the poll at elections. Before the poll it is used to programme ballot modules with poll details or "parameters" which configure the voting machine for use at the poll. After the poll it is used to read-in the contents of the ballot modules, including the votes to be counted. Thus the programming/reading unit is a crucial link in the flow of election information and votes between the election office, the polling station and the count centre.

Approximately the size and shape of a personal computer box, the programming/reading unit has no direct user interface and can only be used in conjunction with a PC on which the election management software has been installed. This is intended to be the hardened PC (see below) but the programming/reading unit can in practice be used with any PC, whether hardened or not and whether or not officially authorised, on which the election management software has been installed.

The programming/reading unit is connected to the communications port of a PC via a serial cable and communicates with the election management software on the PC via a tailored program interface within that software.

A ballot module can be inserted into either of two multi-pin connectors located in apertures in the outer casing of the programming/reading unit. These apertures are identified as the "reading slot" and the "programming slot". Beside each slot is a colour coded key switch which secures the ballot module in place and enables communications between the ballot module and the programming/reading unit. During programming and reading activities, while only one ballot module should be present in the appropriate slot, it is necessary that both keys should be present and operated as described above in order to activate the programming/reading unit.

Each returning officer at the Dáil constituency (service) level[50] uses a programming/reading unit to programme and read-in the ballot modules that are used in the voting machines for which the returning officer is responsible. Nationwide, the ratio of voting machines to programming/reading units is approximately 50 to 1 with each Dáil returning officer having at least one unit per constituency and some having two units, depending on electorate. Including provision for spare units, there are thus approximately 140 programming/reading units in total that would be deployed as part of the chosen system. These are stored locally by returning officers.

Use of the Programming/Reading Unit at Elections

Before the poll, the programming/reading unit is connected to a hardened PC (see *section 3.2.4* below) in the election office of the Dáil returning officer. The election management software (see *section 3.3.2* below) installed on the hardened PC has previously been used by the returning officer

[50] These levels, used for election administration purposes, are described in the context of the election management software in *section 3.3.2* below.

to combine the election data files received from returning officers at European, Presidential, local or referendum levels as appropriate with the Dáil election data file to create a single election data file containing polling options or "parameters" appropriate to each polling centre within the Dáil constituency.

A ballot module is inserted in the writing slot of the programming/reading unit and the election management software is used to programme the election data or "parameters" onto the ballot module that will configure the voting machine designated for a particular polling station within the constituency. This process is repeated for the ballot modules in respect of every polling station in the constituency. The election management software records the ID number of each ballot module programmed for the election and the programmed ballot modules are also labelled.

After the poll, the programming/reading unit is connected again to the hardened PC, either at a local read-in centre within the Dáil constituency or at the count centre for the whole constituency. Each ballot module on which votes have been cast is inserted into the reading slot of the programming/reading unit and the election management software is used to read in (aggregate) the votes and assign (disaggregate) them to vote files according to the different polls that have been held. This process is repeated for the ballot modules in respect of each polling station in the constituency.

(b) Desk Review of the Programming/Reading Unit

The security of the programming/reading unit hardware was investigated by identification and examination of its components and sub-components and by reference to system documentation and other information provided by the Manufacturers. The focus of the investigation was on properties and behaviour of the programming/reading unit that could affect the secrecy or accuracy of an election.

Device Model

The programming/reading unit was firstly modelled as part of a wider model of the whole system. Using this model, the communications and information flows between the programming/reading unit and other components of the chosen system during the respective programming and reading stages before and after polling were identified.

Vulnerability Analysis

A vulnerability analysis of the programming and reading stages was then performed using the HAZOP technique to explore what failures could occur in the communications and information flows between the programming/reading unit and other components of the chosen system, whether they are detected or corrected by design features or if they could propagate to cause undesirable outcomes.

During the above analyses, detailed questions relating to the design and intended behaviour of the programming/reading unit were raised with the Manufacturers, and responded to by them.

(c) Testing of the Programming/Reading Unit

Having regard to the critical functions of the programming/reading unit in configuring the voting machines and handling all of the votes cast in any one constituency, the Commission determined that it would be important to carry out testing of this component of the chosen system. The need for such testing was also highlighted in the Commission's first report[51] which noted that the functionality of the programming/reading unit had not previously been independently tested.

Previous tests of the programming/reading unit carried out by the Commission related mainly to its accuracy in reading in votes. In particular, the input-output volume test of the voting machine described in *section 3.2.1* simulated an election in which large numbers of pre-determined votes were cast and counted and the results checked against the expected outcome.

While this type of "black box" testing demonstrated that the programming/reading unit can accurately process votes on the basis of known inputs and expected outputs, the Commission determined that sufficient proof of the reliability with which it does so could only be obtained from analysis of the C code software embedded within the programming/reading unit. Consequently, the Commission also undertook work in relation to the embedded C code software of the programming/reading unit as described in *section 3.3.1*.

The Commission's further testing of the programming/reading unit for the purposes of this section accordingly concentrated on its secrecy and accuracy properties from a hardware perspective only.

Electromagnetic Susceptibility and Compliance

The programming/reading unit was submitted to tests designed to investigate its susceptibility to electromagnetic eavesdropping and electromagnetic interference. The tests applied were the same as those applied in the case of the voting machine in *section 3.2.1* above. The details and outcomes of those tests are thus applicable to the programming/reading unit also.

Data Security

As described briefly in relation to the ballot module in *section 3.2.2* above, the process of reading data from a ballot module via the serial interface between the programming/reading unit and the hardened PC was monitored. The commands and data exchanged between the programming/reading unit and the PC were then studied.

Volume Testing

A previous input-output volume test of the voting machine described in the Commission's first report[52] confirmed that 36,950 pre-determined votes cast on 739 ballot modules were correctly programmed and read in by the programming/reading units deployed for the purpose of that test.

[51] First Report of the Commission on Electronic Voting, December, 2004: Part 4 p.59; Part 6 p.74; Appendix 2A p.112.
[52] First Report of the Commission on Electronic Voting, December, 2004: Part 2 p.32; Appendix 2C p.167.

The Commission sought to extend its testing of the read-in function of the programming/reading unit in this regard by the introduction of even larger numbers of pre-determined votes to the system by authentic means. However, as already indicated, it was not possible for this purpose either to bypass the user interface of the voting machine or to introduce votes directly onto the ballot module.

The Commission accordingly explored means of entering large numbers of known votes authentically into the system via a test harness designed to bypass both the voter interface of the voting machine and the ballot module as sources of input to the programming/reading unit. It was intended by this means to test the general functions of the programming/reading unit as well as testing its function in reading very large numbers of votes from different ballot modules under different conditions. As indicated above, the importance of this test to the Commission was enhanced by the finding of its first report that the programming/reading unit had not previously been independently tested.

However it did not prove feasible, notwithstanding the cooperation of the Manufacturers, to procure a suitable test harness with which to achieve this and, as further testing of the programming/reading unit itself was not the only objective, this also had a significant impact on the Commission's ability to carry out testing of other hardware and software components of the system further downstream from the programming/reading unit in a substantive and authentic manner.

The Commission's conclusions on input-output volume testing of the programming/reading unit are thus based on the results of the "black box" testing presented in its first report.

(d) Principal Findings Concerning the Programming/Reading Unit

This section sets out the main findings emerging from the Commission's review and testing of the operation of the programming/reading unit from the perspective of the secrecy and accuracy of the ballot.

Hardware Vulnerabilities – Electromagnetic Eavesdropping and Interference

The findings already recorded in *section 3.2.1* in relation to the electromagnetic compliance testing of the voting machine are also applicable to the programming/reading unit. In particular, the programming/reading unit is robust against significant threats of electromagnetic interference or eavesdropping but further testing is recommended.

However, and in the specific context of the use of the programming/reading unit at read-in and count centres when each unit will be critically involved in the processing of all of the votes at a constituency, it was noted that no specific operator guidance is given on positioning the device so as to minimise its susceptibility to electromagnetic threats at elections, whether intended or unintended.

The susceptibility of the programming/reading unit to malicious attack, whether aimed at denial of service or at influencing the result of an election thus needs to be considered in the light of access controls and other physical security arrangements for storage and use of programming/reading units. These arrangements are reviewed in *Part 4* of this report.

Other Hardware Vulnerabilities

As indicated in the Manufacturers' technical description of the system in *Appendix 3*, the programming/reading unit contains the same main electronics board and embedded C code software as the voting machine. This is of particular significance for the secrecy and accuracy of an election because it is further understood from the Commission's work that the voting machine and the programming/reading unit are conceived as essentially the same device, with appropriate interventions and additions being made to its hardware and software configuration during manufacture to determine whether a particular unit will become a voting machine or a programming/reading unit. Arising from this, it is thought that it would be possible, given the relevant knowledge and tools, to adapt a voting machine into a programming/reading unit. If so, this has the implication that an attacker with access to a single voting machine and the appropriate technical knowledge could adapt it to become a programming/reading unit that could be used to program ballot modules. This in turn reinforces the attention that must be paid to arrangements for the secure storage of voting machines, as well as programming/reading units. These arrangements are reviewed in *Part 4* of this report.

Reliance on Embedded Software

In considering the behaviour of the programming/reading unit hardware, it has been assumed that its embedded C code software, and also the Delphi code within the hardened PC that governs its programming and reading functions, operate exactly as expected. Indeed the expected behaviour of the programming/reading unit cited by the Manufacturers in response to various conditions and events suggested in the Commission's analysis is that the device will halt and an error message will be displayed on the election PC.

There is thus a significant reliance on the behaviour of the embedded software that indicates the need for this software to be carefully investigated to establish whether, and how, it protects against hardware failure and other potential vulnerabilities.

Before the poll, the programming/reading unit is critically responsible for configuring the ballot modules and voting machines that are used at the poll and afterwards it is responsible for reading in all of the votes cast in each constituency. This is a particularly important reason to ensure the software behaves as intended since any vulnerability or undesirable behaviour that may be inherent in its design (rather than being maliciously introduced into one or more individual machines) will be present in every programming/reading unit in which the software is installed, causing a potential for system-wide problems.

Software and Hardware Security: Access Controls and Authentication

Although key switches and other physical security features have been applied to the programming/reading unit as described above, no additional security measures such as password or other code protections have been implemented within its software and hardware by which operators must identify themselves before they gain access to its ordinary services while in use before and after polling. Such measures are now commonplace in electronic systems deployed for use in a public setting.

Additionally, in cases where there is an observed failure or other incorrect behaviour of the programming/reading unit a message is displayed on the hardened PC (if connected) and the operator is required to contact a help desk provided by the Manufacturers. Problems are then diagnosed remotely and, where possible, addressed by the operator with remote assistance from a qualified engineer. In cases where a problem with the programming/reading unit cannot be addressed in this way, it must be sent to the Manufacturers for further analysis. It would thus appear that higher levels of access to core services of the programming/reading unit are afforded to system engineers than to election officials at any stage.

The Commission has observed no mechanism within the system that would enable operators, observers and voters to satisfy themselves independently that the hardware and software of the programming/reading unit are authentic and that they are the correct versions that have been tested and certified and that have been approved for use by the electoral authorities. The system is essentially self-checking in this respect.

Data Security

Arising from monitoring of the serial link between the programming/reading unit and the hardened PC, the commands exchanged between the programming/reading unit and the PC were found to be easily discovered and quite straightforward. The protocols for applying check-sums to these commands and to the data stored on the ballot module were also easily discovered. As a result it was found to be possible to extract data from the ballot module in clear text and it was suggested from this work that, given sufficient time, it might also be possible to discover by similar means the data structures necessary to write data to a ballot module.

It was also found to be possible to halt the programming/reading unit by sending it a simple command via a standard PC connected in place of the hardened PC. The programming/reading unit could only be recovered from this state by cycling the power supply.

Volume Testing

As indicated further above in relation to testing of the voting machine, the Commission was unable to exercise the programming/reading unit and other downstream components of the system using large numbers of known votes introduced authentically by bypassing the voting machine interface or by introducing them directly onto the ballot module or the programming/reading unit via a test harness. Although this was a limitation on the Commission’s proposed work, it also represents a strength of the system as it shows that there is a degree of difficulty presented to anyone maliciously seeking to introduce data or votes to the system at an election via the programming/reading unit and/or the ballot module.

General

Although, as indicated above, the voting machine and the ballot module have hardware and software components in common, a significant and critical difference in their respective characteristics concerns the fact that, whereas each voting machine will be responsible for gathering individual votes and storing them together with the other votes cast at a particular polling station (typically several hundred votes per voting machine), each programming/reading unit will be

responsible for reading in the ballot modules containing all or part of the votes for a given constituency (typically in excess of 40,000 votes for a single poll).

There is also a reliance on authorised operators to detect failures of the programming/reading unit hardware or software that may occur while it is being operated, either before or after the poll. Although training in the use of the system will have been provided, which should better enable operators to detect such occurrences, the limited nature of the error messages from the programming/reading unit that are communicated indirectly via the user interface of the hardened PC means that the value of such training may also be limited.

As the read-in of votes from a large number of ballot modules is a critical function that will certainly have a high public profile at election time, the mitigation of any possible failure or other vulnerability of the programming/reading unit will be important in order to maintain public confidence in the system as a whole.

3.2.4 THE HARDENED PC

(a) Description and Use of the Hardened PC

General Description

The hardened PC is used by election officials to run the election management software (see below). It is a standard personal computer to which security measures have been applied to restrict unauthorised access to its services and to its software and data.

As a hardened PC is required by every returning officer to run the election management software, approximately 300 would be deployed at a national election which also included local elections. The hardened PC is stored locally by each returning officer and it is not intended that it should be used for any other purpose between elections or connected at any time to any other computer or computer network.

In order to ensure consistency across all hardened PCs, it is intended that the entire operating system, together with all programmes and data (including the latest version of the election management software and updated anti-virus software) for each PC should be centrally updated by applying a completely new "image" of a standard operational configuration in advance of each use of the PC at elections.

Use at Elections

Before the poll, the hardened PC is used by returning officers at all types of poll (Dáil, European, Presidential and local elections and referenda) to enter election data, including poll and candidate details, into the election management software. It is then used to prepare replica ballot papers for use on voting machines (see above) – these are sent on CD to be printed by a contract printer. The election data file is also copied onto a CD which, except in the case of the Dáil election data file that is retained within the Dáil returning officer's own election management software, is then transmitted to Dáil (service level) returning officers who coordinate the administrative arrangements for taking all of the polls together.

Again, before the poll, the hardened PC is then used by all Dáil returning officers at the service level to read in the election data files received on CD from each other returning officer at European, Presidential, local or referendum levels and to combine these with their own Dáil election data file into a single election data file for all of the polls that will be taken together. The hardened PC is then connected to a programming/reading unit and used with the election management software to programme ballot modules with the details of the combined polls that will be taken at each polling station (voting machine) within each polling centre.

This somewhat complex process arises from the existing administrative arrangements under paper voting at Irish elections whereby polls (i.e. vote gathering) at different types of elections which are conducted simultaneously are coordinated by Dáil returning officers while the responsibility for advance preparations for the poll and for the overall counting of the votes afterwards remains with the European, Presidential, local and referendum returning officer as appropriate in each case.

After the poll, the hardened PC is again connected to the programming/reading unit and is used by Dáil returning officers to read in the election data, now including votes, from the ballot modules that were used in voting machines during the poll. The votes for each type of election are disaggregated by the election management software and assigned to the appropriate vote file for each election. European and local election vote files are then each copied onto a CD which is transmitted to the appropriate returning officer while the Dáil, Presidential and referendum vote files are retained within the election management software at the service level for counting locally by the Dáil returning officer.

Finally, the hardened PC is used by European and local returning officers to read in the vote files received on CD from the Dáil returning officers and, in the case of the European returning officer, the vote files received on CDs from all Dáil returning officers in the European constituency are aggregated into a single file within the election management software. The votes at European and local elections are then counted by the relevant returning officers using the election management software. The votes at Dáil and Presidential elections and at referenda are counted by the Dáil returning officer and the partial local count results of Presidential elections and referenda are reported following each count to the appropriate national returning officer by fax and telephone for incorporation in the overall national count results.

(b) Desk Review of the Hardened PC

It was noted in the Commission's first report[53] that the "hardening" measures implemented to enhance the logical and physical security of the hardened PC were easily bypassed, that the hardened PC was the "weakest link" in the security of the chosen system and that it could thus be used to gain unauthorised access to the election management software and possibly to interfere with the administration or the result of an election.

Having regard to the critical role of the election management software, both in determining the configuration of ballot modules and voting machines before the poll and in reading in, aggregating and disaggregating votes after the poll, the Commission sought to explore further the weaknesses of the hardened PC when used as described above in conjunction with the election management software and the programming/reading unit.

(c) Testing of the Hardened PC

Penetration testing of the hardened PC was carried out in which diagnostic tools, together with hacking tools and techniques were applied to the hardened PC to identify and evaluate its vulnerabilities in the context of use at elections.

The hardened PC was also submitted to tests designed to investigate its susceptibility to electromagnetic eavesdropping and electromagnetic interference. The tests applied were the same as those applied in the case of the voting machine in *section 3.2.1*, with the exception of electrostatic discharge tests and voltage dips and interrupts tests. The descriptions of those tests, but not the outcomes, are thus applicable to the hardened PC also.

[53] First Report of the Commission on Electronic Voting, December, 2004: Part 4 p.56; Part 6, p.75; Appendix 2B p.148.

(d) Principal Findings Concerning the Hardened PC

This section sets out the main findings emerging from the Commission's review and testing of the operation of the hardened PC from the perspective of the secrecy and accuracy of the ballot.

Hardware and Software Vulnerabilities

The penetration testing of the hardened PC has confirmed that the security measures implemented are insufficient to ensure the security of the election management software and sensitive election data:

- not all Microsoft operating system patches have been applied, in particular, the latest patches available since 2003 in respect of security vulnerabilities have not been applied: this would enable a hacker with either network or physical access to use publicly available tools to easily gain administrator access over the hardened PC without requiring any credentials;

- although the hardened PC is not intended for network use and is intended to be deployed in stand-alone mode at elections, it was found that network services were nonetheless available, thus providing a potential avenue of entry into the system by connecting another computer to it: these services were used in conjunction with the security vulnerabilities mentioned above to gain administrator access over the PC;

- user passwords were stored in standard formats within the hardened PC: known weaknesses of these formats were easily exploited using well known hacker tools to obtain the passwords on all user accounts of the election management system, including the administrator account, once administrator level access had been obtained as described above;

- it was found that the smart card facility that has been implemented for login as a normal user was not required for administrator login: thus an attacker who has obtained access and passwords to the system as already described does not require to have a smart card to access the administrator account;

- it was found that the hardened PC would boot from a CD or USB before booting from the hard disc, that the BIOS[54] allowed selection of the boot device during booting and that the BIOS configuration menu was also accessible: it would thus be possible for an attacker to load their own operating system and other software on the PC and to add, remove or interfere with data;

- the anti-virus software was found to be ineffective against the specific and well known hacker tools installed on the hardened PC and used during testing as described above to identify system passwords: although the software examined the files that had been installed on the system, it did not report them as malicious.

The electromagnetic compliance testing of the hardened PC indicated that there is a small vulnerability to denial of service attack at the nuisance level in respect of electromagnetic interference but that this can be mitigated by appropriate location of the equipment away from

[54] Basic Input/Output System.

potential threats. However, it was also noted that no specific operator guidance is given on the location of the device so as to minimise its susceptibility to electromagnetic threats at elections, whether intended or unintended.

When considered in the context of the security characteristics of the election management software discussed further below, the critical role of that software in determining the accuracy of all other components of the system, and the limited protections implemented by that software in respect of sensitive election data, including votes, it is clear that the hardened PC in its present form, in combination with the election management software, constitutes a significant weakness within the chosen system that requires to be addressed through review and enhancement of its security measures.

3.2.5 USE OF COMPACT DISCS (CDS)

(a) Description of Use of Compact Discs

Compact discs are used to transmit information to, from and within the chosen system in the following ways:

- updated versions of the election management (Delphi code) software are supplied to returning officers on CD;
- replica ballot papers prepared within the election management software (and which are placed under the voter's panel of each voting machine at elections) are transmitted in PDF format on CD to contract printers for colour printing;
- election data files prepared within the election management software are transmitted on CD between returning officers at various levels before the poll at an election or referendum;
- files containing votes cast are transmitted on CD between returning officers at various levels after the poll at an election or referendum.

Updated Versions of Election Management Software

It has been noted in *Part 4* of this report that updated versions of the election management software are provided by the Manufacturers to the Department by e-mail. Multiple copies of the software are then prepared for distribution to returning officers on CD, together with instructions as to how it should be loaded onto their hardened PCs. It has also been noted previously that different versions of the software could be installed and remain simultaneously resident on a single PC.

An alternative method by which the election management software can be updated involves the "ghosting" onto the hard disc of each hardened PC of an image which includes the entire operating system, election management software and other software and hardware configuration information and programs, including anti-virus protection appropriate for use at a particular election. This process would be coordinated centrally before each election and the requirement to issue a further update of the election management software to returning officers on CD would only arise in circumstances where the software was updated in the run-up to an election but after the PC "ghosting" process had been completed in respect of that election.

It might also be considered necessary between elections to provide returning officers (and others) with updated versions of the software on CD for training and evaluation purposes, etc. Version 139 of the software was provided in this way to the Commission for the purposes of its work.

Replica Ballot Papers for Printing

The arrangements for polling at all elections of all types and at referenda (including the programming of ballot modules in respect of combined polls and the set-up and administration of

voting machines at polling centres) is coordinated at a "service level" by Dáil election returning officers as described in *sections 3.2.4* and *3.3.2* of this part. However each individual returning officer at Dáil, European, Presidential and local election levels and at referenda remains responsible for arranging the printing of the replica ballot papers that will be used in the voting machines deployed at the poll by the Dáil returning officer.

Taking into account the types of poll that are likely to be taken simultaneously, and while the replica ballot papers for Presidential elections and referenda are the same across all constituencies, there are in excess of 270 different types of replica ballot paper to be printed in the case of local elections (268 local electoral areas) coinciding with a European election (4 constituencies) and a Presidential election and/or a referendum.

In practice, and in view of the high levels of security, quality, accuracy and consistency that are required, the printing of replica ballot papers is coordinated by the Government Supplies Agency so that only a small number of regional printing centres are involved, each responsible for printing replica ballot papers for a number of returning officers. Each of these printing centres will thus receive a large number of CDs containing different replica ballot papers from different returning officers. Once printed, the replica ballot papers are delivered to the appropriate returning officers for checking prior to being transmitted to Dáil returning officers for use on voting machines at the election as described in *section 3.2.1*.

Election Data

In parallel with the production of replica ballot papers as described above, each individual returning officer at all types of elections and at referenda is also responsible for preparing an election data file within the election management software in respect of the poll that will be conducted for their constituency. This file contains the date and description of the poll and the constituency and the names and details of the candidates.

Returning officers at European, Presidential and local elections and at referenda then transmit this election file on CD, together with the printed replica ballot papers, to the Dáil returning officer at the service level who coordinates the arrangements for the taking of the poll.

Each Dáil returning officer uses the election management software to combine the election data files received on CD from (typically) one European returning officer and from (typically) several local returning officers, together with the election data file for the Dáil election (if any) within their own constituency. From this a combined election file is generated which reflects the several possible permutations of Dáil, European and local election types in respect of which a poll is being held within the Dáil constituency. This combined file is then used to programme ballot modules via the programming/reading unit as described in *section 3.2.3*.

Vote Data

Following the poll at a combined election, the Dáil returning officer at the service level uses the election management software and the programming/reading unit as described in *section 3.2.3* to read in and aggregate the votes in respect of different polls as recorded on all ballot modules within the constituency. As they are read in, the votes on each ballot module are first disaggregated into separate vote files for each poll. When all votes have been read in, the vote file for each poll is

copied onto a CD and transmitted to the relevant local or European election returning officer for counting. The votes at Presidential elections and referenda are retained and counted locally by Dáil returning officers with the local count results being transmitted by fax and telephone to the central count centre at national level for incorporation into the overall count.

Identification and Authentication

The CDs proposed for use in the transfer of election data are type CD-R used in a manner that allows only one write of data. Thereafter the CD is read-only. Data in XML format is saved to the hardened PC before it is written to CD and a second copy of the CD is made as a backup in the event of destruction, loss, etc., of the original.

At the 2004 elections it was proposed to use coloured labels on the exterior of the CDs in order to distinguish between the CDs for each type of election. Provision was made for key information to be recorded on the labels, including a unique serial number, relevant poll details, date, time and the signature of the returning officer.

It was also proposed that a hard copy of the data should be provided with the CD when it is being transferred between returning officers at different levels so that the data could be verified when received.

(b) Desk Review of Use of Compact Discs

While there are security concerns surrounding the transmission of election software and replica ballot papers on CD before an election as described above, the Commission's main concerns relate to the transmission of sensitive election data, including votes cast, between returning officers on CD in the course of an election.

The principal vulnerabilities associated with the use of CDs as the transmission medium for such sensitive data relate to the generic CD technology and data formats that are deployed and to the absence of any significant security measures to prevent or detect malicious or accidental access to the data which could result in its alteration or corruption.

A further vulnerability relates to the numbers of different CDs that will be travelling in different directions at around the same time and the numbers of CDs, all of similar general appearance, that will require to be handled simultaneously in locations, particularly at read-in and service centres operated by the Dáil election returning officers and at count centres operated by European election returning officers.

Unlike the locked ballot box formerly used to transmit unused ballot papers (before the poll) or used ballot papers (after the poll), the use of the CD as a transport medium and the data formats proposed within the chosen system are significantly less secure and, being also less visible and transparent than ballot boxes, they are significantly more vulnerable to deliberate or accidental loss, damage or alteration of their contents. Given the widespread availability of CD technology, they are also readily susceptible to replication and substitution.

(c) Testing of Use of Compact Discs

Given the potential vulnerabilities identified above in respect of the CDs and data formats proposed for the transfer of sensitive election information, and given also the vulnerabilities identified in *section 3.3.2* below in respect of the election management software which is responsible for reading and writing the data transmitted via CD, the Commission sought to examine possible methods by which these vulnerabilities might be exploited.

The following tests were accordingly carried out:

- A CD containing an election file (such as might be transmitted by a local election returning officer to a service level returning officer before the poll) was examined to see whether the election details it contained could be altered.

- A CD containing a vote file (such as might be returned by a service level returning officer to a local election returning officer after the poll) was examined to see whether the votes it contained could be altered.

These tests were carried out in conjunction with the testing of the election management software described in *section 3.3.2*.

(d) Principal Findings Concerning Use of Compact Discs

In general it was observed that, while the protections on the physical security of data contained on CDs and on ballot modules were broadly similar in terms of ease of access, the more rigorous housekeeping measures implemented in respect of ensuring the integrity and availability of vote data stored on the ballot module were absent in the CD. This point is significant when it is considered that, while each ballot module will contain the votes that have been cast on a single voting machine, a CD may contain all or part of the votes that are cast in an entire constituency (typically in excess of 40,000 votes).

The tests carried out by the Commission indicated that it would be possible to access data, including votes, transmitted on CDs and to alter the data without detection:

- election data files on CD are not protected and vote data is not sufficiently well encrypted to prevent unauthorised access: the use of public/private key cryptography would protect the data from being read if it were intercepted;

- data, including votes, on CD is not cryptographically signed to prevent unauthorised alteration: the use of public/private key cryptography would protect against attempted access and against malicious or accidental alteration of data while stored on CD.

Although a form of encryption is applied to vote data on CDs, confidence in the secrecy of the ballot would be greatly enhanced if the data was protected from unauthorised access and disclosure by the cryptographic security measures mentioned above, which are standard ways of protecting any sensitive electronic information. Such measures can be implemented in a way that is transparent to users and operators of voting equipment and that will not impact on its simplicity or ease of use.

There are thus significant hardware and data security vulnerabilities associated with the use of CDs, in the manner currently proposed, to transmit sensitive election data, including votes, between election offices, service centres, read-in centres and count centres at elections. Little mitigation in respect of these vulnerabilities is provided either by the formats in which data is currently recorded onto the CDs or by the election management software which is responsible for writing and reading this data. Better protection could be provided by the implementation of enhanced data encryption measures and by the cryptographic signing of data transferred on CDs.

Rigorous management control of the flow and use of the many CDs containing sensitive election data that are exchanged between returning officers at different levels is also critical to the accuracy of any election conducted using the chosen system. A significant error in this regard could compromise the entire system. There is therefore a reliance on the administrative procedures and physical security arrangements for the deployment of CDs as part of the chosen system at elections. These matters are discussed in *Part 4* of this report.

3.3 Review of Software Components

This section describes the general features and proposed use of each main software component of the chosen system, the analysis and testing of each component carried out by the Commission and the principal findings of that work.

Appendix 1 contains an overview and illustrations of the main components of the chosen system and a description of its proposed operation at elections in Ireland. *Appendix 3* contains a description of the technical features of the chosen system provided by the Manufacturers for the purposes of the Commission's work.

Approach to Analysis

The source code of the embedded C code and Delphi software of the chosen system, together with related documentation, was made available by the Manufacturers for examination to a trusted third party working on behalf of the Commission. As indicated in *Part 2*, the Commission's approach to the investigation of the software was a phased and structured one whereby progression of the work to each successive stage was largely dependent on the results of the previous one.

The design and development of the software was first reviewed by reference to the documentation supplied by the Manufacturers, by audit of further documents and through meetings with relevant personnel, where possible, at the Manufacturer's premises in Holland.

The quality of the implementation of the software was then investigated by direct examination of the source code leading to the development of a functional model, the identification of critical components and the identification of possible areas of concern.

Software Engineering Standards

Each software component was considered in the context of the high standards of software engineering that would be expected of a mission critical system such as the chosen system. As indicated in *Part 2*, it is very important in this context that the code not only does its specified job, but that it has been developed in a rational way and in accordance with expected standards for mission critical systems. Not only must mission critical code appear, when viewed as a black box, to do its job, but it must also be well documented, well structured and navigable so that it is possible for independent reviewers and programmers to understand it, maintain it, update it and extend it when necessary.

The standards applied by the Commission in reviewing the software may be summarised as follows:

- All code is clearly written and fully commented.
- Behaviour of the code is consistent across the whole source code.
- There is a well-documented software project management plan.
- There is good quality documentation on properly followed development procedures including requirements capture, design, implementation documents, configuration management

documents, unit/integration/system testing documents and quality assurance documents (including review and verification/validation activities undertaken).
- Source code is kept under rigorous version control.
- A specific standard of coding style is documented and followed.
- The structure of code is logical, follows from design documents, is broken down hierarchically if necessary, and exhibits a clear separation of concerns.
- Areas of possible problematic behaviour (such as potential divide by zeros, failing system or utility calls, array indexing, casting, pointer arithmetic, memory leaks) are well documented as well as clearly and explicitly avoided.
- All other systems that are relied on by the software meet similar quality requirements.

Additional expectations that raise confidence in the quality of software are an automated issue management system and some recognised certification for the developers.

If the systems by which computer code is developed meet most of these requirements, this indicates that the code has been developed in a manner appropriate to a high-quality system. The code will be well documented and structured, and thus relatively easy to understand and evaluate. This in turn means that maintaining and upgrading the code is likely to be a straightforward and reliable process.

However, if many of these standards are not met, this points to the code (and the processes used to develop the code) as being somewhat impenetrable, likely not to be of a high standard, and thus unsuitable for a mission-critical application. This in turn may mean that future detailed analysis and evaluation of the code would have to be extensive, as there can be no *a priori* confidence in the software, given the system of work by which it was developed.

The source code of the Delphi and C software components of the chosen system, together with supporting documentation, provided by the Manufacturers were thus investigated in order to acquire insights into whether or not these standards are met. Features of the code that were examined for this purpose included software documentation, code comments, code implementation, code style, code architecture and version control.

During the above analyses, detailed questions relating to the design and intended behaviour of the software were raised with the Manufacturers, and responded to by them.

3.3.1 EMBEDDED SOFTWARE (C CODE)

(a) Description and Use of Embedded Software (C code)

Installation, Configuration and Use

The embedded C code software is installed at the time of manufacture on the voting machine and programming/reading unit hardware components of the chosen system. Since the primary function of the embedded C code software is to control the operation and use of these hardware devices and the ballot module as already described, it is not necessary to describe its functions here.

While the functions of the C code software are largely internal to the voting machine and the programming/reading unit, there are in effect two user interfaces. In the case of the voting machine, the software interacts with voters via the voter's panel and with election officials via the control unit and the voter's panel. In the case of the programming/reading unit, the software does not have a direct user interface via the programming/reading unit itself but interacts indirectly with election officials via the election management software running on the hardened PC.

The voting machine contains three separate types of board, each running its own specific executable programs created from a separate source code. These types of boards are: the voting machine main board; the connection board; and the display board. The programming/reading unit contains only one type of board; as noted in *section 3.2.3*, this is the same as the main board of the voting machine.

Furthermore, while the source codes of the connection board and the display board are separate entities, the voting machine main board shares its source code in common with the programming/reading unit main board as both devices are conceived as a single entity.

The embedded C code is thus split up into three parts: the main board code, controlling either the voting machine or the programming/reading unit; the connection board code; and the display board code of which there are 5 copies, one for each display board that is associated with a column of preferences on the voter's panel of the voting machine.

Functionality

The system-level functionality of the different elements of the C code is as follows:

The main board code on the voting machine controls the following:

- configuration of the voter's panel of the voting machine, i.e. reading candidate information from the ballot module and displaying it on the voter's panel;
- the control unit used by the operator to determine the mode of the voting machine;
- LCD displays on the voter's panel and control unit indicating, as appropriate, voter preferences and error messages;
- recording and storage of votes as they are cast by voters; and
- transfer of votes onto the ballot module and backup module.

The display board code controls the following:

- monitoring of the voter's panel buttons for key presses and passing their addresses to the connection board; and
- displaying a voter's selected preferences via LED displays.

The connection board code controls the following:

- passing of requests from the main board to the display board;
- passing of information and key press addresses received from the display board to the main board; and
- generating error messages if more than one button has been pressed at once or a key has been pressed for too long.

The main board code on the programming/reading unit controls the following:

- writing of the candidate information onto the ballot module before the poll; and
- reading of the votes from the ballot module after the poll and passing them to the hardened PC for counting.

(b) Analysis of Embedded Software (C code)

Design and Documentation

The embedded C code was considered by examination of the documentary evidence to identify the processes that were used in its design and development. During this review, evidence was sought that activities including requirements capture, modelling, design, coding and testing had been carried out and documented to an adequate standard.

Code Analysis

A code analysis of the C code was then carried out in three stages.

Firstly, an inspection of the code was carried out to determine the structure and functionality of its different components. This inspection was performed without the use of any documentation so that the analysis could be wholly independent. Each of the three main parts of the code was inspected separately, followed by a study of their interactions to understand how they link together in the system. The software was thus effectively reverse-engineered from the source code. A functional model of the C code was created as a result of this work, together with some metrics relating to its size and complexity.

Secondly, those functions of the code that were considered to be critical in terms of secrecy and accuracy were identified from the functional model. The criticality of a function was based on the overall role it performed, together with findings from the analysis of hardware components described above and which highlighted behaviour of the system that was critically dependent on functions of the code.

Thirdly, an automated search of the code was carried out using a proprietary analysis tool to identify distinct types of potential run-time error that can occur in C code. This tool returns a "concern" for each potential error identified and further manual investigation is then required to "discharge" these concerns, some of which can be false. This manual investigation of concerns is beyond the scope of the Commission's work for the purposes of this report.

General

The analysis carried out assumed that the code as provided was the correct version as installed on the ESI2 voting machine and on programming/reading units deployed for use in Ireland and that it was unaltered from the code used for compilation. The analysis related only to the C code itself and did not consider either the compiler used to produce the executable program from the code or the reliability of the processor or operating system.

It is also important to note that the existence of a concern arising from the automated search of the code using a proprietary analysis tool does not necessarily indicate the presence of a run-time error. It merely indicates that the program is not "well behaved". It is likely that many of the concerns raised in this way may, in further analysis, be discharged as "false concerns", having factored in all the possible inputs to the system.

(c) Testing of Embedded Software (C code)

Unit and system testing of the critical components of the C code had been planned, if considered necessary and appropriate, as a later part of the Commission's overall phased approach to software assurance of the chosen system as described in *Part 2*.

However, having regard to the fact that the C code analysis described above, and the findings further below, represent the Commission's first opportunity to consider the C code component of the chosen system, and having regard also to the issues that have arisen from the Commission's work in relation to other components of the chosen system, it was considered neither necessary nor appropriate for the Commission to carry out any formal static or dynamic "glass box" testing of the C code at this time.

The Commission nonetheless sought to carry out some dynamic "black box" testing of the C code and of the system as a whole by introducing and processing large numbers of known votes through the system. However, and as described above in relation to the various hardware components of the system it was not possible either to bypass the user interface of the voting machine or to introduce votes directly onto the ballot module or via the programming/reading unit to achieve this objective.

(d) Principal Findings Concerning Embedded Software (C code)

General

The review of the design and development of the C Code suggests that there is evidence that a recognisable structured design process has been used but there has been insufficient independent review and testing within this process.

The code analysis did not uncover any functional failures. However the analysis was only partial and activities performed, together with the observations made, suggest that more detailed analysis is required before it would be possible to conclude unambiguously on the integrity of the C code.

Software Quality

Having regard to the software engineering standards that would be expected of high quality mission critical software identified above, the following are the specific observations that have arisen from the Commission's work in relation to the C code:

- The clarity of the code is adequate, although some parts are easier to understand than others.
- Much of the code's behaviour appears to be consistent, with functionality common to two of the three parts being implemented in a similar manner. However, the consistency of the third is patchy.
- A software quality plan was made available. However, it was not easy to gather sufficient evidence of a good development process from an audit of the available documentation.
- Some useful documentation has been supplied on the design, specification, development and quality of the software. A small discrepancy between the specification and the detailed software design was observed.
- Version control appears inadequate as the version numbers are not common across the code and the procedure to find and change the embedded version number is not documented, which means it cannot be quickly or easily checked.
- No documentation concerning coding style appears to exist and no evidence was found in the code of any recognisable standard being followed.
- Overall, the comments contained in the C code are patchy: in some places they are clear and accurate, whilst in others they are inadequate for the functionality of the code to be understood.
- One of the three parts of the code is logically structured, with sensible functional layers. The remaining two parts are less so, but justifiably so because the functionality of the code in these parts is less complex.
- The automated analysis found no potential divide by zero errors, but did find a significant amount of other potential run-time errors present in the code. The significance of these can only be determined by further analysis and it is likely that many of them will be discharged as false concerns.
- The software does not rely on external software to accomplish its goals, although it is closely coupled to the election management software (Delphi code) which is, in turn, reliant on the Windows operating system of the hardened PC (see below).

Architecture

The incorporation, within the C code on the main board, of functionality relating to both the voting machine and the programming/reading unit represents an inadequate segregation of functions. A consequence of this is that either function may be susceptible to changes made in the other and both would have to be re-tested as a result of any such change.

Further Work and Analysis Required

As can be seen from the Commission's consideration of the embedded C code – especially given the reliance, already noted, of the voting machine, ballot module and programming/reading unit hardware on the behaviour of the C code software – further analysis, investigation and testing, and possibly amendment of the C code will be required.

Much more confidence in the code could be gained through the updating and re-evaluation of the documents describing the functionality of the code. This would ensure that the behaviour of the software is more accurately described.

In addition, because the completion of this activity would involve comparing the functionality of the code with that described in the documents, the code itself could in turn be checked for correct functionality.

Confidence in the correct functioning of the code could also be gained through improvements to the quality and quantity of comments and through improved version control. Coding errors would then also be less likely to occur in future maintenance and enhancement activities.

A better picture of the quality of the C code could be gained by completing the second (manual) part of the automated analysis of concerns carried out by the Commission. This is done through the discharging of the concerns raised during the automated analysis.

Following these activities, it would be worth applying some simple checks on the healthiness of the code, such as more indicative code metrics and perhaps the verification of the code against its specification.

Testing

In regard to testing of the C code component of the chosen system:

- The possibility of "glass box" testing of the C code proved unnecessary at this time in light of the Commission's findings in relation to other components.

- Given the lack of suitable test harnesses for inputting large numbers of known votes into various points of the system, it was not possible within the context of this report for the Commission to carry out the high-volume "black box" testing of the C code that would ideally be desirable.

- Both types of testing of the C code will however be necessary following any changes that may be made to the system in the future, whether as a result of the Commission's conclusions or otherwise.

- Extensive testing of the C code will, in any case, be required before any proposed use of the chosen system at elections in Ireland.

Specific Concerns

While it is possible for the Manufacturers' engineers to corroborate that check-sums of the executable C code software file reported by a voting machine printout as being installed on that voting machine are correct, it is not readily possible, nor is it required by prescribed procedures, for operators or others to confirm independently that the version of the C code installed on the voting machine or the programming/reading unit is the correct version and to verify that it has not been altered. Ideally, it would be desirable to have a procedure for the same independent body that tested and certified the software generally to confirm also its correct installation on each voting machine and that there should be a feature within the system to support this form of independent verification.

A further potential vulnerability may exist in that a feature of the system designed to facilitate voting by visually impaired persons in other applications of a similar voting machine outside Ireland remains present within the C code software. Taken with the existence of a physical external data link within the voting machine hardware (also present but not currently proposed for use at Irish elections), there is uncertainty as to the degree to which the functioning of this feature has been deactivated in a way that prevents any intended, or possibly unintended, use.

3.3.2 ELECTION MANAGEMENT SOFTWARE (DELPHI CODE)

(a) Description and Use of Election Management Software (Delphi Code)

Installation and Configuration

The Delphi code software component of the chosen system is an integrated election management software application provided by the Manufacturers on CD or by e-mail. It is installed in the hardened PC (or on any other PC) and is used by election officials to manage all election data, including votes, for polls in which the chosen system is deployed.

The election management software comprises a Windows-based user interface with underlying data processing and storage functions. It is used before the poll to enter election and candidate details and to programme ballot modules via the programming/reading unit. After the poll it is used to read in, aggregate and count the votes and to compute the results.

Functionality

The election management software has been designed to take account of a number of specific features of the polls that take place in Ireland:

- the types of polls held include parliamentary (Dáil Éireann), European Parliament, Presidential and local government elections, together with constitutional referenda;
- the electoral method and count rules employed at elections are proportional representation/single transferable vote (PR/STV);
- polls for more than one type of election or referendum may be taken simultaneously;
- overall responsibility for electoral policy, including electronic voting, rests with the Department while polls are administered locally in the first instance by returning officers at local (268), Dáil (42), European (4) and Presidential/referendum (1) constituency levels;
- when different types of poll are taken simultaneously, administrative responsibilities are coordinated in a layered manner between returning officers for each type:
  - before the polls, the returning officers each receive candidate nominations and prepare the ballot papers in respect of their own constituencies,
  - the polls are then conducted by the Dáil returning officers as a "service level" who coordinate the preparations made at all other levels and gather the votes,
  - after the polls, the votes are returned to the appropriate constituency levels for counting by the respective returning officers and announcement of the results.

There is thus a considerable degree of complexity involved in implementing an electronic system to replicate the current administrative arrangements under paper voting. As noted above, much of this arises from the possibility of holding several different types of poll simultaneously, each with a different returning officer but with coordinated arrangements for the gathering of the votes.

The overall configuration of the election management software for this purpose within the chosen system involves the physical movement of many ballot modules and CDs between election offices, polling centres, read-in centres and count centres. As such, the election management software acts

as a "data hub" within the chosen system – a distributed system whose various components are not connected by physical data links – and there are many such hubs in the context of the nationwide deployment of the chosen system as described below.

Although implemented in a different language from the embedded C code software of the voting machine and programming/reading unit, the election management (Delphi code) software has been designed to interact with the programming/reading unit via a program interface:

- This program interface enables the election configuration data entered by election officials into the election management software to be written to the ballot module via the programming/reading unit.

- This program interface also enables the votes cast by voters using the voting machine to be read from the ballot module via the programming/reading unit.

Based on a prototype presented by the Manufacturers at the procurement stage, the election management software was developed by way of an iterative process of refinement and review between the Department and the Manufacturers, to meet these and other prescribed requirements[55] of the Irish electoral process, including statutory requirements.

The election management software accordingly includes specific functionality for conducting each type of poll that may occur at Irish elections, together with functionality for carrying out the different tasks that may be required at each constituency level when multiple polls of different types are taken simultaneously. The software also includes an implementation of the count rules used to count votes at Irish elections.

Use at Elections

For the purposes of illustration, the following are the activities carried out by the respective returning officers at each constituency level in the context of use of the election management system at simultaneous Dáil, European and local elections. Similar arrangements would apply if Presidential elections and referenda were included in various possible combinations with these three types of election.

Before the Poll

Returning officers at all three constituency levels (Dáil, European and local elections) use the election management software on a hardened PC in their election offices to create an election file containing the poll details (election type, date, constituency, etc.) and details of nominated candidates (name, description, photograph, party logo) for their respective election.

They then arrange the printing of the replica ballot papers that will be used on the voting machines as described above. Returning officers at local and European level then copy the election file onto a

[55] Request for Tenders Document of the Department (June 2000), Count Requirements and Commentary on Count Rules and Updates Nos. 1-7 thereto. These documents are available at *www.cev.ie/htm/tenders/info_tenders.htm.*

CD and send it, together with the replica ballot papers, to the Dáil (or "service level") returning officer.

European level constituencies are larger than Dáil constituencies and local level constituencies are smaller than Dáil constituencies. A European level returning officer thus sends the same election file on CD to all Dáil returning officers within the European constituency while a Dáil returning officer receives a different CD from each local level returning officer within the Dáil constituency.

The Dáil returning officers then use the election management software at their election offices to read in and combine the election files for the local and European elections for which they are responsible with the election file for their own Dáil constituency. The resulting file becomes the election file for the combined poll.

In this example, the details of the European and Dáil election ballots will be the same throughout the Dáil constituency whereas the local election ballots will vary across different local electoral areas within the Dáil constituency.

Each Dáil returning officer then connects their hardened PC to a programming/reading unit at their election office and programs ballot modules with the appropriate poll data or "parameters" for each of the polling stations (voting machines) within each polling centre in their constituency. The ballot modules are then inserted into voting machines while the corresponding replica ballot papers are placed on the voter's panel of each voting machine as described in *section 3.2.1*.

During the Poll

On polling day, Dáil returning officers deploy the voting machines for use by voters at polling centres as described in *section 3.2.1*. European and local returning officers are not involved in this process.

After the Poll

Each Dáil returning officer is responsible for the removal of the ballot modules from the voting machines and the transportation of these to the Dáil election count centre (or, in some larger constituencies, to a "read-in" centre) where they are inserted into a programming/reading unit connected to a hardened PC and the votes they contain are read into the election management software.

As the votes from each ballot module are read in, they are disaggregated according to election type and added to the appropriate Dáil, European or local election vote file within the election management software. When all the ballot modules have been read in, the vote file containing the votes for each European and local election is copied to a CD and sent to the appropriate European or local returning officer for counting.

Each European and local returning officer loads the vote file from the CD onto their hardened PC.

Returning officers at all three constituency levels then use the election management software on their hardened PC to count the votes and announce the result of the election in respect of their constituency.

Audit

During the counting process, records can be printed out or saved electronically to indicate the steps taken and the results at each stage of the count.

In the event that an election is subsequently questioned by way of an election petition and a full or partial recount is ordered by a court as permitted by law, it is also possible to print out all the ballots, together with an indication of how they were numbered following their initial mixing and which numbered ballots were randomly selected for transfer during the count. The transfer history of each individual ballot is also recorded. The conduct of the count can thus be verified by the court.

Software Versions

While all types of poll have been provided for in various combinations within the election management software and can also, in theory, be conducted individually, not all single polls or possible combinations of poll have currently been provided for. The software is described by the Manufacturers as being under continuous development and it is accordingly envisaged that the version to be used for a given poll combination will be produced specifically for the purposes of that poll when it becomes necessary.

(b) Analysis of Election Management Software (Delphi Code)

Design, Development and Documentation

The Delphi code was firstly considered by examination of the documentary evidence to identify the processes that were used in its design and development. During this review, evidence was sought that activities including requirements capture, modelling, design, coding and testing had been carried out and documented to an adequate standard.

Code Analysis

A code analysis was then performed on version I-1.00 build 0139 of the election management (Delphi code) software as provided by the Manufacturers. The analysis has assumed that the code as provided is the correct version – there is nothing obvious within the code itself to indicate this – and that it is unaltered from the code used for compilation. The analysis is only valid for this version of the code since, if the code is changed or has incremental alterations, the observations made may no longer be valid.

The aim of this code analysis was to produce a functional model of the software, identifying its critical functions and detailing the links the software has to the rest of the system. From this analysis, a number of potential vulnerabilities have been identified, comments have been made on the basis of an inspection of the code and recommendations have been made on further analysis that may be required.

The approach taken was to analyse the source code directly in the first instance so that an understanding of it could be developed independently of any associated documentation. The

analysis was carried out in two stages.

Firstly, through a combination of manual and automatic source code analysis, a functional model was created, showing data flows between the units and functions within the software.

Secondly, the functional model was analysed to identify the critical functions of the Delphi code, the critical inputs and outputs and some metrics relating to its size and complexity. Certain types of potential error that were suggested from the modelling of the code were also considered at this stage.

Navigation and inspection of the code during both these stages also facilitated the identification of vulnerabilities and protections within the source code and the gaining of an overall impression of its structure and quality. This impression was then compared with the expectations of high-quality software, as described above, to obtain a view of the code quality.

Critical Functions

In terms of the classification of the criticality of the Delphi code functions, a procedure is classified as critical if its misbehaviour could adversely affect an election result. The critical procedures of the Delphi code can thus be categorised into three broad groupings:

- importing/exporting data, including votes,
- counting votes,
- presenting information and results.

The procedures within these groups are not specific to individual votes – they deal with larger collections of votes – and so any incorrect behaviour could in all likelihood affect all of the votes dealt with by that procedure. Therefore the majority of procedures in the Delphi code have been classified as critical.

Furthermore, given its role in configuring the ballot module with the election data or "parameters" that will be used to configure the voting machine and its role in reading in, aggregating, disaggregating and counting the votes cast, the election management software is critically involved both before and after the poll at an election because all other hardware and software components of the chosen system are dependent on its correct functioning.

(c) Testing of Election Management Software (Delphi Code)

Previous Testing by Commission

Previous testing of version 131 of the election management software using 10,000 election test cases as described in the Commission's first report[56] highlighted an error in the counting algorithm. This error was subsequently addressed in version 139 of the software as supplied for the purposes of the analysis described above and the Commission accordingly sought to confirm that the error was no longer present. The tests necessary to confirm this were carried out as part of the further testing of the count algorithm described below.

[56] First Report of the Commission on Electronic Voting, December, 2004: Appendix 2E, p.201.

Testing of Count Algorithm

The Commission extended its previous testing of the election management software in which 10,000 election test cases were counted in parallel by the count algorithm of the election management software and an alternative count algorithm developed for the purpose of the Commission's work.

Over 100,000 election test cases were accordingly prepared involving both large and small numbers of candidates, large and small numbers of votes and large and small numbers of preferences, together with test cases based on ballots cast at real elections and test cases designed to exercise the count algorithm in unusual counting situations that might arise in unexpected or unanticipated ways.

Testing of Access Controls

In the course of carrying out penetration testing of the hardened PC as described further above, the security measures of the election management software that runs on the PC were also considered. As the physical and software security measures implemented on the hardened PC were found to be inadequate, increased emphasis is placed on the protections within the election management software itself, not least because it has been specifically designed so as to be capable of use on any Windows based PC without the implementation of any specific additional security measures.

Testing of Data Security and Integrity

The Commission conducted a mini-election to examine the measures implemented within the software to ensure the security and integrity of election data, including votes. Although no secrecy issues arise in this context, it was considered that the integrity of this data was the single greatest determinant of accuracy within the chosen system, given the critical role played by the software in determining the configuration of ballot modules, voting machines and replica ballot papers before the poll and in reading in, aggregating, disaggregating and counting the votes after the poll.

Other Testing and Certification

As currently proposed, the software is undergoing continuous development and it is intended that a new version of the software will be issued prior to each use of the system in Ireland. Each new version will take account of the particular polls that are to be taken simultaneously and other distinguishing features of the election. Given this process of continuous development, it would be critical to have in place a rigorous system for independently testing, verifying and certifying the version of the count software that is actually deployed in any given election. Such a system does not currently appear to be envisaged.

The Commission had sought to test the performance of the software by running Dáil, European and local elections concurrently. However it was not possible to test this combination of polls as such a combination is unlikely to arise in practice and it has not been included in the software. The Commission accordingly tested the software as described above by running a European election and two local elections simultaneously.

(d) Principal Findings Concerning Election Management Software (Delphi Code)

General

Arising from the source code analysis, no major functional failure has been found in the election management software. However, a full analysis has not been performed, merely the reverse-engineering of the system to enable a functional breakdown, identification of critical code and highlighting of some quality indicators.

A failure has however been identified in testing of the count algorithm of the election management software as described further below.

The development of the software and its adaptation for use in Ireland do not appear to have been underpinned by a full and formal process of requirements capture and specification. Analysis of the design and development processes has identified little evidence to support a claim that the software is dependable and little documentation to support this claim was available. Significant areas where the documentation is incomplete are the design processes and evidence of testing.

During the code analysis, several features of the code were noticed which are not consistent with the standards of software engineering that would be expected of high quality mission critical software indicated above.

Software Quality

Having regard to the software engineering standards that would be expected of high quality mission critical software identified above, the following are the specific observations that have arisen from the Commission's work in relation to the Delphi code:

- The code is not well structured: it has a flat layout with little hierarchy, contrary to all tenets of good coding practice.

- The behaviour of the code does not appear to be consistent. For example potential divide by zero operations are not all protected; the protections applied are not all consistent and in some cases appear to have been applied at a later date as a batch job that may not have been completely thought out.

- A software project management plan was not supplied – it is questionable whether one exists.

- No useful documentation has been supplied on the design, specification, development or quality of the software. Design documentation (at least) appears not to exist.

- There is some question as to the effectiveness of any version control procedures being applied to the software development.

- No documentation concerning coding style appears to exist. No recognisable coding standard appears to have been followed.

- The code is not well commented: code that has been commented out is present without explanation, temporary comments exist and there is little commenting on the intended behaviour of functions and units.

- The code does not appear to use either abstraction or separation of concerns, which ease both understanding and future maintenance.

- The code has some questionable characteristics. The function of its exception handling is not clear (and an exception may cause the database to end up in a malformed state); the statements containing real divide operators have protection that may not be appropriate; and some potential divide operations do not have any protection.

- Although the election management software does not appear to rely on external software to accomplish its goals, as a Windows application running on the hardened PC it relies on Microsoft Windows for resource allocation, scheduling, user interface and access to peripherals. The Microsoft Access 97 database has also been extensively integrated within the election management software for the purposes of data storage and handling.

Additionally, the development does not seem to have followed any industry standards with regard to software development, or to have any certification that could add to confidence in the software integrity.

The features identified above do not point to definite errors in the functionality of the election management software. However, they do undermine confidence in its integrity. In some respects, these features point to areas for further analysis (for example the divide by zero issues), and suggest ways in which the software could be improved (for example, separation of concerns and the addition of comments).

Accuracy Issues

In terms of accuracy requirements, a number of the issues raised previously may affect the accuracy of elections both directly and indirectly:

- The structure of the code and the lack of documentation may mean that implementation errors stay hidden.

- Code has been found that has no functional effect.

- It is unclear as to whether other similar code exists that should have a functional effect.

- Specific areas for concern are the handling of potential divide by zero errors and other exceptions that may affect the accuracy of election results.

Further Work and Analysis Required

The current findings thus suggest that much further analysis is required before confidence can be gained in the integrity of the election management software. This may not in practice be achievable,

given the apparent lack of documentation.

Certainly the potential accuracy issue with the divide by zero handling requires further analysis, and other areas of implementation that could impact negatively on accuracy may still exist and require detailed analysis to identify and characterise the risks.

Full analysis of the software may not be possible without a specification of what its behaviour should be. However it is not clear whether such a specification exists in an appropriate, formally controlled document.

Given the apparent immaturity of the software there is also a requirement for evidence of changes in development procedures, full commenting of the code, and documentation of the full software development, maintenance and testing process.

Consequently, given that there were doubts about the design and development process, and since several minor failings had already been identified before detailed functional analysis took place, it is questionable whether the integrity of this software can be sufficiently assured for use in a real election without significant modification, documenting, analysis and testing.

Testing of Access Controls

The security measures within the election management software were found, in the course of penetration testing of the hardened PC, to be inadequate. Although access to the software requires users to login, it was found that the login passwords are given in the help page that is available prior to login.

Furthermore, although the Microsoft Access databases used by the election management software to store election details and results are password protected, these passwords are stored within the software itself and can be extracted with relative ease, thus allowing the election details and results to be accessed and edited at will.

Testing of Count Algorithm

Arising from the functional testing of the election management software described above, a number of concerns have also arisen, including the identification of an error in the count algorithm.

It was found, when the results of the 100,000 election test cases described above were compared with the results produced by the alternative count algorithm developed for the purposes of the Commission’s work, that the election management software had produced the same result as the alternative implementation in the vast majority of cases. However there were a small number of cases that were counted incorrectly.

In these cases, it was found that in circumstances where a number of candidates are tied and it is necessary to determine which candidate should be eliminated, the election management software makes an incorrect determination as to which of the tied candidates should be selected for this purpose. The action taken by the election management software as a result of this determination may cause a candidate to be incorrectly eliminated, thus affecting the outcome of the election.

A further issue with the election management software was also indicated as a result of examining the error described above. It was noted that, in addition to selecting the incorrect candidate for elimination, the software makes a further error by reporting incorrectly through its user interface that a different candidate has been selected. Thus the error in selection is compounded by an error in reporting the selection.

While it was not feasible, given the very large number of possible election permutations, to exhaustively search every election scenario, it is likely that further errors may also exist in the count algorithm of the election management software.

Testing of Data Integrity and Security

Arising from the investigation of the protections on the integrity of data within the election management software, a number of significant and important vulnerabilities were identified.

Firstly, it was found, when reading in votes at a count centre from a CD received from a service centre, that it is possible to read in the votes from an incorrect service centre. It was also possible to read in votes from the same service centre twice and those from another service centre not at all. This suggests that there are no checks carried out within the software to ensure that the data, including votes being read in, are attributed to the correct source and are read in once and once only, thus placing unnecessary reliance on administrative procedures to detect and recover from any such error. If such an administrative error were to remain undetected, as seems possible, the accuracy of the election result could be compromised.

Secondly, it was found that, if an election data file was amended after a previous version of the file had already been issued to service centres, the data returned from the service centre based on the previous version could nonetheless be read in to the amended file. This suggests that there are no checks carried out within the software to ensure, for example, that election data, including votes, are attributed to the correct candidates and that such an error could easily go unnoticed. Again, the accuracy of an election could be compromised if such an error remains undetected.

Thirdly, and most significantly, it was found possible to manipulate vote data by directly editing entries in the election file stored in the Microsoft Access database within the election management software. This was found to be possible at both the service centre and count centre levels without detection by the software. This is a crucial shortcoming in the software since it is possible by this means either to disrupt an election or, in any case, to change the outcome. Such interference could occur either maliciously or accidentally, with potentially serious effects on the accuracy of the election.

These findings amplify the Commission's finding in *section 3.2.5* that rigorous management control of the flow and use of the many CDs containing voting data that are exchanged between returning officers at different levels is critical to the accuracy of any election conducted using the chosen system.

Implications of Test Findings

The emergence of these concerns regarding the functional behaviour of the election management software is consistent with the concerns recorded further above in relation to the quality of this

software arising from the Commission's review of its design and development stages and the analysis of its code implementation. Of further concern is the possibility that other deficiencies of the software may also exist but that these may remain hidden in parts of the code that are not readily amenable to testing.

Additionally, it is a fundamental design shortcoming that the election software is being continuously developed, with a new version issued as a matter of course in advance of each new election or set of combined elections. This means that all new versions of the software, as noted above, will require rigorous re-testing and re-certification. If the software continues to be undocumented and opaque to analysis, then all re-testing to investigate the effect of such changes is likely to be expensive and time-consuming and/or ineffective.

Alternative Approaches

The cost of the further analysis and testing that is necessary in respect of the election management software, and the requirement for repeated analysis and testing in respect of future releases of the software, must be weighed against the cost of implementing an alternative system.

In terms of quality and reliability, the use of controlled open-source software is one possible option that has a number of advantages:

- visibility of the election system code would act as a strong motivator to write clean, well-commented code;
- by making the election system code readable by the world, a large amount of free analysis is performed, and history shows that any issues with the code's accuracy would be discovered quickly;
- the available resource base for future development and support is broadened;
- the counting process is no longer contained within a black box: it is open for all to inspect.

In outlining these features of open-source software development methods, the Commission is not advocating the adoption of such methods in any future development of the chosen system but is rather highlighting the benefits that may be derived from broadening the development base and adopting alternative approaches to development methods.

For example, an intermediate approach would be to have the software developed by a well-defined development team but to make it widely available for open review at appropriate stages before, during and after development.

3.4 Testing

This section presents a composite overview of the testing work carried out by the Commission, the details of which have already been described in previous sections of this part in the context of the Commission's work in relation to individual hardware and software components of the system.

It is important to re-emphasise that the tests carried out by the Commission were not intended to prove or demonstrate the fitness for use of the chosen system (although some of the tests carried out would be appropriate for this purpose). The primary purpose of these tests was to assist in the Commission's investigation of various properties of the chosen system and, in particular cases, to identify or confirm properties of the system the existence of which could not readily be ascertained by analysis or other methods of investigation.

3.4.1 TESTING CARRIED OUT

(a) Testing of Hardware

Electromagnetic Surveillance and Disruption Testing

The voting machine, the programming/reading unit (both containing ballot modules) and the hardened PC were submitted to tests designed to investigate their susceptibility to surveillance and disruption by electromagnetic means and also to variations and interruptions in the mains power supply. Additionally, the electromagnetic compliance tests carried out previously in respect of the voting machine and programming/reading unit were reviewed in the context of their use at public elections. The findings based on the results of these tests in relation to the voting machine, ballot module and programming/reading unit are described at *sections 3.2.1*, *3.2.2* and *3.2.3* respectively above, while those in relation to the hardened PC are described at *section 3.2.4*.

Penetration Testing

The programming/reading unit and the hardened PC on which the election management software is installed and run were submitted to tests designed to investigate the security of the programming/reading unit and the hardening measures implemented in respect of the hardened PC. These tests were carried out while the hardened PC was reading and writing data via a serial connection to a programming/reading unit containing a ballot module. The findings based on the results of these tests in relation to the security of the ballot module and programming/reading unit are described at *sections 3.2.2* and *3.2.3* above while those in relation to the hardened PC are described at *section 3.2.4*.

Use of Compact Discs (CDs) - Data Security and Integrity

Recognising the widespread reliance within the chosen system on the use of CDs to transfer sensitive election data, including votes, between election offices, service centres, read-in centres and count centres, the Commission sought to investigate the security of the methods implemented

within this process to protect the data. In particular, the transfer of election data files on CD before the poll and the transfer of votes on CD after the poll were selected for testing. These tests were carried out as part of the data security and integrity testing of the election management software. The findings in respect of the use of CDs based on the results of these tests are described at *sections 3.2.5* and *3.3.2* above.

Usability Analysis

In the course of the Commission's investigation, review and testing of the chosen system, a number of usability issues, relating principally to use of the voting machine by voters, were identified that could have a bearing on the secrecy or accuracy of an election. The results of this analysis are described at *section 3.2.1* above.

(b) Testing of Software

Election Management Software: Count Algorithm

The Commission's previous testing work[57] highlighted an error in the implementation of the Irish election count rules within the count algorithm of version 131 of the election management software. The Commission sought to establish that this error had been addressed in version 139 as provided for the purposes of the Commission's further work. The Commission extended from 10,000 to 100,000 the number of election test cases (with known votes) used to exercise the count algorithm in parallel tests with the alternative count algorithm developed for the purposes of the Commission's previous testing. The findings based on the results of these tests are described at *section 3.3.2* above.

Election Management Software: Data Security and Integrity

As the election management software is critically involved in configuring all other hardware and software devices within the chosen system with data before and during the poll, and as it is also critically involved in the handling and counting of votes after the poll, the Commission sought to investigate the data security and integrity measures implemented within the software.

A mini-election was accordingly prepared using the election management software to configure separate polls which would be conducted simultaneously. Details of each poll were prepared separately, transferred onto CD and then combined into a single election file at a service centre. A programming/reading unit was then used at the service centre to programme ballot modules with the combined polls and these ballot modules were inserted into voting machines. A small number of known votes were cast using the voting machines. The votes were then read in from the ballot modules, disaggregated into vote files for each election and transferred onto CD. The votes for each election were then imported into the election management software where they were counted. The findings based on the results of these tests are described at *section 3.3.2* above.

[57] First Report of the Commission on Electronic Voting, December, 2004: Part 2, p.30; Appendix 2E, p.201.

3.4.2 OTHER TESTING

(a) Additional Testing Planned by Commission

Volume Tests of Hardware and Embedded Software (C code)

During previous end-to-end volume tests of the chosen system carried out by the Commission and involving the manual entry of large numbers of known votes at a single election, the entry of vote data via the voting machine user interface was found to be cumbersome, slow and subject to user-error in the entry of known vote data. This method of data entry was thus deemed unsuitable for the purposes of extended further testing of the system as envisaged by the Commission.

The Commission accordingly sought to obtain access to, or to develop, test harnesses which would variously bypass the user interface of the voting machine, bypass the voting machine itself or bypass the ballot module for the purpose of entering very large numbers of known votes into the system at different points so as to test the downstream components and functions of the system.

The intended purpose of this testing was to thoroughly exercise the entire system in an authentic manner, particularly those component parts and functions at the boundaries of other components (such as the vote read-in function of the programming/reading unit) identified by the Commission's earlier reports as not having been tested previously.

Notwithstanding the cooperation of the Manufacturers, it was not possible within the timeframe and other parameters of the Commission's work to obtain, adapt or develop suitable test harnesses for this purpose. This operated as a significant constraint on the Commission's ability to test aspects of the chosen system in a way that would complement the other analysis and review work being carried out. The effects of this constraint are described in relation to the voting machine, the ballot module and the programming/reading unit at sections *3.2.1*, *3.2.2* and *3.2.3*, respectively, above.

Open Testing of the System

The Commission also considered whether it would be possible, in the interests of greater transparency regarding the proposed use of the system in Ireland, to provide an open interface so that members of the public and other interested parties could interact with the software of the system via the Internet. In this way, it would be possible for anyone to set up test elections, enter votes and have them counted in a realistic manner using the actual software components of the chosen system, accessed through a simulated hardware interface.

A further development of this concept, also considered by the Commission, was to offer interested parties the opportunity, given the relevant parameters and a suitable on-line interface to the hardware components, to develop their own implementations of the software against which to test the validity of the chosen system as an implementation of its identified requirements and specifications.

Although recognising that such approaches would provide useful testing of the system and could

also serve to meet the significant public interest in the system recorded in the many submissions[58] received by the Commission in the context of its earlier reports, it was decided that such a process lay somewhat beyond the scope and timeframe of the Commission's immediate brief to consider the secrecy, accuracy and testing of the chosen system.

(b) Previous Testing by Commission

In view of the fact that it was not feasible, as described above, for the Commission to carry out the volume testing of the system that it would have wished to, many of the findings and conclusions from the Commission's work in this report are accordingly based on an input-output volume test carried out previously by the Commission.

This test, described in the Commission's interim and first reports presented in April and December 2004, involved the casting and counting of 36,950 known votes across 739 voting machines at a single election.

Together with the other tests carried out by the Commission for the purposes of its previous reports, this test also remains valid for the purposes of this report.

(c) Review of Official and Independent Testing

The Commission is required by its terms of reference to review the tests already undertaken to validate the chosen system. However, as the Commission has not been advised of any further official or independent testing of the chosen system that has been carried out since the time of its previous reports, the Commission's views in relation to such testing remain at this time as they were presented in those reports.

(d) Further Testing Required

Further development and testing of the chosen system will be required in order to meet the findings, conclusions and recommendations of the Commission's work as presented in this report. A significant consideration in this regard will be the degree of independence of any body that is engaged to carry out testing or certification of the system or its component parts, both during and after such developments.

Although the carrying out of substantive testing or verification of the system lies beyond the scope of the Commission's remit, future testing of the system, and the evaluation of its general amenability to rigorous independent parallel and end-to-end testing, will be informed by the tests carried out by the Commission and also by those tests that the Commission sought to carry out, but was unable to for reasons outlined above.

All of the testing carried out by the Commission for the purposes of this report has been carried out in respect of the current hardware and software versions of the components of the chosen system and their interaction as a whole system. These tests, together with any tests carried out by others to confirm various behaviour and properties of the system would have to be repeated in respect of any

[58] First Report of the Commission on Electronic Voting, December, 2004: Part 3 and Appendix 3.

future version of the system that might be proposed for use following the introduction of a new version of any individual hardware or software component.

3.5 Conclusion on Technical Aspects and Testing

This section sets out the Commission's conclusions arising from its work in relation to technical aspects and testing of the chosen system as described in the previous sections of this part. The Commission's conclusions arising from its work in relation to other aspects of the chosen system are set out, in each case, at the end of the other relevant parts of this report. The Commission's overall conclusion on the chosen system is set out in *Part 7*.

On the basis of its consideration of technical aspects and testing of the chosen system[59], as described in this part, the Commission concludes as follows:

HARDWARE

The main hardware components of the system, namely the voting machine, the programming/reading unit and the ballot module are of good quality and design. They are robust against failure and are well suited to their purpose. Further investigation, refinement, testing and independent certification of these components would however be necessary before they could be recommended for use at elections in Ireland. Specific areas for improvement include user access controls and device authentication measures on the voting machine and programming/reading unit and data integrity and security measures on the ballot module.

The measures implemented to secure the hardened PC on which the election management (Delphi code) software would be installed and used to configure elections and to count the votes are inadequate and would need to be reviewed and strengthened in light of the Commission's conclusion further below regarding that software.

The Commission's work has indicated improvements, many of which involve only relatively minor modifications or additions to the system, that would be necessary in order to address these issues before the main hardware components of the system can confidently be used at elections in Ireland.

SOFTWARE

The embedded C code software within the voting machine and programming/reading unit is of an adequate standard and, while it is not of mission critical standard, there is evidence to suggest that it has been developed according to a recognisable structured design process that is broadly in accordance with industry best practice. Further investigation of its behaviour, followed by refinements of its functions, further testing and independent certification would be necessary before its reliability could be confirmed beyond reasonable doubt for use at elections in Ireland. Specific areas for attention include those aspects of the software that govern the user interface of the voting machine and those that govern data security measures on the programming/reading unit and ballot module. These issues can be easily addressed by modifications to the software itself.

The election management (Delphi code) software installed on the hardened PC and used to prepare elections and to aggregate and count the votes has not been developed in accordance with any

[59] The main components of the chosen system referred to in these conclusions are illustrated for reference in *Appendix 1*.

recognisable standard process and is thus unlikely to be capable of meeting the high standards of software engineering that would be required in a mission critical system. Design weaknesses, including an error in the implementation of the count rules, that could compromise the accuracy of an election have been identified and these have reduced the Commission's confidence in this software.

This finding is significant in view of the critical role of the election management (Delphi code) software in configuring all of the other hardware devices and peripherals within the system at elections and its role in handling all election data, including votes. Furthermore, the fact that errors have been found in those parts of the software that have been examined and tested by the Commission raises the question of whether errors may also exist in other parts of the software that are less amenable to such examination and testing.

Given the Commission's findings about the inadequacies of the development process for the election management (Delphi code) software, and the functional errors and other weaknesses that continue to emerge it is unlikely that this software could be feasibly amended to enable its reliability to be confirmed. Accordingly, the Commission does not recommend the use of the election management (Delphi code) software at elections in Ireland but notes that it is likely that alternative election management software, compatible with the hardware and embedded C code software of the system, could be developed at a reasonable relative cost.

PERIPHERALS

While the ballot module is robust and generally well suited to its purpose, the measures for ensuring the security of the sensitive data stored on it could be improved by the implementation of enhanced data security measures to give greater confidence in the integrity of the system.

The widespread use of CDs, in the manner currently proposed, to transfer sensitive election data, including votes, between centres is not sufficiently secure and represents a potential risk to the accuracy of elections. The use of CDs in this context and the application of appropriate security measures should be rigorously reviewed and strengthened in the light of the Commission's conclusions above in relation to the election management (Delphi code) software and the hardened PC.

The Commission has recommended data encryption and cryptographic signing of data as measures that can enhance the integrity and security of votes contained on ballot modules and CDs. Such measures can be implemented in ways that are transparent to users and operators of the chosen system and that will not impact on its simplicity or ease of use.

SECURITY

The measures provided within the system as a whole to restrict access to its services, to enable operators and observers to check that the software and hardware versions are correct, and to protect against unauthorised access and/or alteration of data (including software and votes), are less rigorous than would be appropriate for the protection of sensitive data in a mission critical system.

There is, as a consequence, heavy reliance on the integrity of administrative procedures for the

secure deployment of the system. It is desirable that greater protection against unauthorised access and interference should be afforded by the system itself in the first instance, including by means of enhanced access controls and independent software and hardware verification procedures.

These issues can also be addressed by relatively minor modifications or additions to the existing components of the chosen system.

TESTING AND INDEPENDENT VERIFICATION

The testing of the system as a whole carried out to date, as well as the investigation, analysis and independent testing and certification of its individual components, is insufficient to provide a secure basis for the use of the system at elections in Ireland. There is thus a need for comprehensive, independent and rigorous end-to-end testing, verification and certification by a single accredited body of the entire system as proposed for use in Ireland. While the Commission's work has laid the foundations for this process, more work will be required in this area.

CONTEXT OF THESE CONCLUSIONS

These conclusions on technical aspects and testing of the chosen system have been drawn, and should be interpreted by others, in the context of the Commission's conclusions arising from other aspects of its work set out elsewhere in this report. This includes the Commission's work on physical and operational security aspects of the chosen system (*Part 4*) and the comparative assessment of the chosen system and the paper system (*Part 5*). These conclusions are also incorporated within the Commission's overall conclusion on the chosen system in *Part 7*.