Part 2

Work of the Commission

Introduction (*Part 2*)

This part introduces and provides an overview of the Commission's work which is presented in detail in *Parts 3* to *6* of this report. The scope of the work is described in *section 2.1*, the standards of secrecy and accuracy adopted by the Commission are defined in *section 2.2*, the Commission's approach to the work is described in *section 2.3* and an overview of the work is given in *section 2.4*. Relevant aspects of the commencement, management and conclusion of the work are described in *sections 2.5* and *2.6* while *section 2.7* places the Commission's work in the context of wider electronic voting developments.

2.1 Scope of the Work

Role of the Commission

The Commission's terms of reference require it to do the following:

- consider the secrecy and accuracy of the chosen system,
- review the testing carried out and carry out its own further tests, and
- carry out a comparative assessment of the chosen system and the paper system of voting,

and these requirements have accordingly informed the scope and direction of the Commission's work as introduced in this part.

The Commission has had no involvement in the decision to adopt e-voting in Ireland or the steps by which this decision has been implemented to date. These events largely preceded the Commission's establishment in March, 2004 and the Commission has not been asked to consider them (although the requirements and specifications for the system have been considered as part of the Commission's remit).

Responsibility for policy and ongoing administration of electronic voting thus remains a matter for the Government and the Department in conjunction with returning officers.

Testing and Validation

Responsibility for official testing and overall validation of the system is also a matter for the Department. The Commission has not been specifically asked to test, prove or conclusively verify the chosen system, but rather, in the context of reporting on its secrecy and accuracy, it is authorised by its terms of reference to review the tests already carried out and to carry out its own further tests.

Analysis of the software of the chosen system, together with some further testing of individual components and functional testing of the system as a whole, has accordingly been carried out by the Commission on this basis in the context of this report. As no further official testing of the chosen system has been carried out by the Department, the main work carried out by the Commission in regard to reviewing the previous tests of the system is contained in its first report[8].

[8] First Report of the Commission on Electronic Voting, December, 2004: Parts 2 and 4.

2.2 Standards of Secrecy and Accuracy

One of the first issues that the Commission had to address was to identify the standards of secrecy and accuracy that it should apply in its consideration of the chosen system. In fact these standards have remained unchanged since the Commission's previous reports and they also largely precede the adoption of electronic voting in Ireland.

Secrecy

Secrecy of the ballot is required by the Irish Constitution and has been held by the Courts in *McMahon v Attorney General*[9] to mean that the ballot is secret to the voter - "complete and inviolable secrecy" and includes the particular requirement that it must not be possible for the voter to prove how they have voted. Acknowledged subsequently in sections 137 and 162 of the Electoral Act 1992 which impose obligations of secrecy on persons present at the issue of ballot papers or at the opening of ballot boxes, this standard of secrecy has also been adopted by the Commission in its work.

In adopting this standard, the Commission notes that the Courts have also held that persons who require assistance in voting are regarded as "electing to waive their constitutional right that this vote should be completely secret". This does not mean that secrecy is no longer a requirement in the case of such voters but, rather, that the level of secrecy they enjoy is necessarily reduced to facilitate the exercise of their right to vote. The Commission has accordingly taken the view that the highest technically feasible levels of secrecy should be afforded to such voters, who include persons with disabilities and persons with literacy difficulties.

The Commission acknowledges that this concept of secrecy does not relate to the disclosure of the intentions or actions of persons intending not to vote either by abstaining or deliberately spoiling their vote. The use of the chosen system by such persons has nonetheless arisen for consideration in parts of the Commission's work, namely, in reviewing the design, intended behaviour and usability aspects of the voting machine as the principal user interface of the system and also in comparing the overall functionality of the chosen system with that of the existing paper system.

Accuracy

Although the Commission did not find it necessary to define a precise standard of accuracy for the purposes of its earlier reports, it determined that accuracy related to matters concerning the demonstrable integrity and consistency of the methods for the gathering of the votes at polling stations, the methods for the translocation of the votes from polling stations to count centres, the process of disaggregating groups of votes for counting in different types of elections and the methods for counting and distributing votes.

Electronic processing systems can, when functioning correctly, achieve standards of accuracy that are considerably higher than the equivalent manual systems. In a critical process such as voting at national elections, it is to be expected that the highest possible standards of accuracy (i.e. closely

[9] *McMahon v Attorney General* [1972] IR 69, (1972) 106 ILTR 89.

approaching 100%) should be achieved in the electronic recording, handling and counting of votes and this is the standard that has been adopted by the Commission in its work.

In addition to the near-zero error rate that this standard implies in terms of computational accuracy, any electronic voting system and the arrangements for its deployment must also incorporate measures designed to prevent, or at least minimise to the greatest possible extent, any influence on accuracy caused by human error in the design or operation of the system. The Commission has also adopted this requirement for the purposes of its work.

Other Standards

The Commission also adopted other relevant technical and operational standards as it saw fit for the purposes of its work, including in its own methodology for carrying out the work. Where these are recognised standards, they have been identified as such in the relevant parts of this report while, in other cases where it has been necessary for the Commission to determine its own standards, particularly in the area of software engineering, the relevant requirements have been specified in each case in the light of current best practice and expectations of electronic voting systems generally.

2.3 Approach to the Work

Overall Approach and Principles

In approaching its work, the Commission took a broad view of the chosen system. Analysis and testing were clearly carried out during the development of the chosen system and, subsequently, following its adaptation for use in Ireland[10]. Different parts of the system were reviewed by different independent bodies, both within Ireland and internationally, each having its own expertise and perspective in relation to particular aspects. However none of these bodies was asked to take a view of the chosen system as a whole, incorporating all relevant aspects of its hardware and software components, its physical environment and the operational arrangements for its use.

This led the Commission to take a broad view of the system within the particular scope of its terms of reference. In taking this broad view of the chosen system, the Commission has had regard to the following key principles:

- any system is more than the sum of its component parts: In addition to considering its component hardware, software, physical and operational aspects, any review of an electronic voting system must also consider how these aspects fit together and interact. Thus, for example, the security features of any voting machine as a hardware device cannot be considered in isolation from the operational security arrangements for its use at elections and the physical and logical security measures to restrict and detect unauthorised access to the voting machine and its services both at and between election times;

- any system is only as strong as its weakest link: The ability to record votes with perfect accuracy will be undermined if there is a potential for error in the counting software; the value of protections afforded by a secure voting machine and a secure counting process will be diminished if the manner of transferring votes between these processes is not also secure; and the value in implementing high levels of security around voting machines on polling day will be diminished if they can be tampered with when stored between elections.

The Commission's work has thus sought to investigate the hardware, software and physical security features of the chosen system in combination with the operational arrangements for its deployment at real elections in Ireland, with significant findings from each strand of the investigation informing the other strands. An overview of this work is provided in *section 2.4*.

Software Assurance

A particular focus of the Commission's work at all stages since its establishment has been on the software of the chosen system. The Commission's previous reports[11] highlighted the requirement for independent review and testing of the software in order to provide the necessary assurances that it is reliable and can be confidently recommended for use in Ireland. However it was not possible within the timeframe of those reports for the Commission to take significant steps in this direction.

While the provision of this type of assurance in a substantive way does not fall within the

[10] First Report of the Commission on Electronic Voting, December, 2004: Appendix 1B p.83.
[11] First Report of the Commission on Electronic Voting, December, 2004: Part 6 p.74 and p.78.

Commission's role, the steps that can provide preliminary indicators regarding the reliability of the software of the chosen system have now been taken by the Commission. This was made possible within the context of the enhanced levels of access to the documentation and source code of the system permitted by the extended timeframe of this second report.

Software Quality

As the chosen system relies substantially on the correct functioning of its software to achieve its purpose and, in order to demonstrate that it achieves that purpose with the requisite levels of secrecy and accuracy, it is necessary to investigate the quality of this software.

The case for establishing the secrecy and accuracy of the system as a whole is thus substantially reliant on establishing that the software is well written and can be relied upon to do its job properly. Translated into software engineering terms, this requirement is expressed in terms of the need to assure the "trustworthiness" of the software by confirming, with reference to its prescribed requirements, specifications and other indicators, that it behaves as intended and displays no unintended behaviour.

While it is difficult to quantify measures of "trustworthiness" for this purpose, other criteria such as reliability, availability (robustness), usability, transparency, auditability, integrity (security), correctness (conformity) and functionality (operation) are more clearly understood and can provide useful indicators and measures of quality in relation to software engineering. These terms, together with other relevant indicators, are accordingly used in this report.

The concept of "trustworthiness" as a technical term also aligns closely with the concerns about the chosen system that have been raised in the public and political debate and by individual voters, including the many people who made submissions[12] to the Commission regarding the proposed use of the system in 2004. Given the reduced transparency of electronic voting processes when compared with paper voting, these voters clearly seek assurance that the system will record, include and count their votes accurately while also maintaining the high level of secrecy that they are accustomed to under the paper system. Thus it is the same property of the system – the reliability of the unseen workings of the software – that needs to be assured in order to satisfy the concerns of users, critics, observers and reviewers of the system alike.

With a view to establishing the quality of the software that is responsible for ensuring the trustworthiness of the chosen system as a whole, the Commission has identified the following software engineering aspects for consideration:

- documentation;
- design and development processes;
- source code.

The Commission's approach to identifying the appropriate software engineering standards to apply in the case of the chosen system is discussed further below while detailed consideration of these aspects of the software of the chosen system is set out in *section 3.3* of *Part 3*.

Recognising that the cost of "building in" software quality in these areas must be balanced against

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

the potential cost in the event of failure of the software to meet its purpose, the Commission also considered the role of the software of the chosen system in the light of the potential consequences of such failure.

Quality Standards for Electronic Voting Software

While it might seem that administering elections and recording, aggregating and counting votes is not a very taxing challenge for computer systems, there is no doubt that the role of any electronic voting system in determining the results of national elections leading to the formation of parliaments, governments and other branches of national and local administration is a "critical" one in terms of confidence in the democratic process and the potential effect those outcomes can have on the social and economic well-being of a state and its citizens.

A useful analogy referenced by the Commission in this regard is the development by a major commercial bank of new electronic banking software to handle its on-line banking services, ATM transactions and customer accounts - an application that offers some similarities to electronic voting:

- the underlying counting tasks are fundamentally very simple but very important;
- these tasks have been performed manually for many years to most people's satisfaction;
- the processes involve manipulating large amounts of sensitive data;
- similar types of data are input from many different sources;
- data is secret and its accuracy is required to be maintained;
- key user interfaces are provided in a very public setting;
- the system must avoid failure or error due to both honest and dishonest manipulation;
- localised small failures can be tolerated but systematic failure would be very serious;
- widespread failure of the system can affect the well-being of individuals and of society as a whole.

Key differences between electronic voting and electronic banking which raise the required standard for electronic voting software even higher include the following:

- the outcome of electronic voting determines the formation of the government of a sovereign state and, unlike a banking system, a system failure can never be fully retrieved since re-running an election on a different date creates a completely different political context;
- electronic voting systems are used and operated by persons who only do so at widely spaced intervals rather than on a daily basis and who will therefore be less familiar with them;
- secrecy is not an express requirement in the design of an ATM or on-line banking interfaces in the same way as it is a requirement at Irish elections;
- if the users of banking services are dissatisfied with the system in one bank, they have the option to move to another bank.

It thus appears reasonable to the Commission to suggest as a benchmark that at least the same or higher standards of quality assurance should be provided by the State to its citizens in introducing an electronic voting system as a major bank would require when introducing a new electronic banking system.

Critical Systems

Having identified the role of electronic voting as a critical one, it was necessary for the Commission before commencing its work to decide *how* critical the chosen system is in order to determine the appropriate quality standards to apply in reviewing it.

The classification of critical systems can be expressed in terms of the economic or human cost of failure. At one end of the criticality spectrum are "safety critical" systems where failure may lead to loss of life, injury or damage to the environment. At the other end of the spectrum are "business critical" systems where the cost of failure is purely financial, albeit very significant to the business as a whole and to its reputation. Between these categories are "mission critical" systems where there is no direct threat to life or limb but where the cost of failure is likely to directly threaten the well-being of individuals or groups who rely on the system but who were not necessarily responsible for its failure.

While, in certain circumstances, a threat to the secrecy of an individual vote may be life-threatening, it is difficult to reason that an electronic voting system should be classed as safety critical in the context of its use in a mature democratic electoral process such as exists in Ireland. Certainly the cost of development associated with safety critical applications such as nuclear reactor control systems, space travel or automatic pilot systems for aircraft would render electronic voting economically unfeasible.

At the other end of the spectrum, the failure of an electronic voting system is clearly business critical, at least in the sense that it will be costly financially, and in terms of reputation, at the electoral administration level to re-run elections or to recover from failures during them. At the democratic, social and economic levels however, the worst case scenario would be where the system fails to elect the correct candidates, possibly resulting in the incorrect formation of a government. Although there is no meaningful way of equating this kind of failure with a financial cost, its adverse impact on the well-being of individuals, society and the State is potentially great. Electronic voting is thus more critical than systems such as those used in point of sale, accounting, data handling, stock control and other wide-scale business and administrative applications, even though commercial pressures and the potential consequences of failure would cause considerable investments of effort and money to be made in the development of such systems also.

On this basis, the Commission determined that, having regard to the democratic, social and economic consequences of failure in a system that would be deployed in the critical tasks of recording and counting votes at public elections, the levels of quality software engineering that are necessary to ensure that the overall goals of secrecy and accuracy are met by such a system are those applicable to mission critical systems.

System Architecture

A particular characteristic of the chosen system identified by the Commission in this regard concerns the architecture of the system as a whole and how its individual components relate to each other in the context of its deployment within and across constituencies at elections.

The chosen system is involved in the following activities when multiple polls take place at the same time:

- at election offices: generating poll data files for different election types;
- at service centres: combining poll data files received from different election offices into composite poll data files;
- at polling stations: recording votes for each election type simultaneously;
- at read-in centres: reading in and aggregating the votes received from polling stations and disaggregating them into partial vote files for each election type;
- at count centres: aggregating the partial vote files received from read-in centres into composite vote files for each election and then counting the votes.

On this basis, the Commission views the chosen system as a distributed system, with complementary tasks being carried out at distributed processing centres using common parameters such as poll configuration data which is transmitted between centres as appropriate, together with variable data such as votes.

However, and in contrast to the distributed geographical configuration of its individual components, there are no physical or other connecting links between the components of the system although it operates in a way that enables them to share and exchange data as though they were connected. This involves the exchange of data between centres using portable media, i.e. ballot modules and CDs. The data exchanged by these methods is managed mainly by the election management software.

This virtual connectivity and sharing of data thus relies significantly on the deployed methods for exchanging and handling data between centres (i.e. the ballot module, CD and election management software) and places considerable emphasis on the integrity, robustness and suitability of those methods to fulfil their intended purpose.

Engineering Standards for Electronic Voting

Having determined that electronic voting is a mission critical application, it was then necessary to determine the engineering standards that might be expected to have been applied in the development of the chosen system, and whether the application of these standards can be identified from quality reviews of the hardware and software development processes, documentation and the source code.

Critical Systems Engineering

There are three main aspects of critical systems engineering where such standards play a role:

- hardware standards ensure that design and manufacturing errors cannot lead to failure and that the likelihood of components reaching the end of their “natural life” does not compromise the reliability of the system;
- software development standards ensure that the probability of failures due to errors in specification, design and implementation is reduced;
- operations standards reduce the likelihood that humans make mistakes when interacting with the system, and that when human error does occur the system can cope with it.

In order to apply these standards in a demonstrable and provable manner, the Commission considered the chosen system in different ways, each having regard to the criticality of the system as a whole. This included reviews of the hardware and software of the system, its physical security

and the administrative arrangements for its deployment as described in *Parts 3* and *4* of this report. An overview of this approach is provided in *section 2.4* of this part.

Central to this review are the election management software and the embedded software of the chosen system. These software components have been specifically examined with regard to the indicators of quality provided by their documentation (including requirements and design specifications), the design methodology used in their development and the source code central to the design implementation.

Quality Assurance

In carrying out its work, the Commission also had regard to different approaches that can be taken to assuring quality in the design and development of computer systems.

One such approach involves the aggregation and analysis in a meaningful manner of the views and knowledge of customers, users and other interested parties, together with problem-domain experts, to develop a clear and structured view of the intended system in terms of its intended purpose (requirements specifications) and design. This "human-oriented" approach is usually most meaningful when undertaken before the development starts. When it has been undertaken, this also provides useful evidence that a quality process has underpinned the requirements capture and design specification stages of the system.

As the Commission has had no role in the development of the chosen system, this approach was largely not open to it, although consideration was given to the available documented requirements and specifications deriving from the development of the system and its eventual selection. In the case of the chosen system, these requirements specifications are contained in public documents[13] of the Department and the Manufacturers concerning the procurement process for the chosen system and also in private documents of the Manufacturers relating to the original design of components of the system (which preceded its procurement) and their adaptation for use in Ireland. These documents were provided to the Commission for review.

A more "technology-oriented" approach to analysis involves examination of the system, its components and the overall quality of the finished product. This can be carried out retrospectively (i.e. after the development) by systems engineering experts and without the strict need for domain experts. This approach is based on the principle that the quality of engineering involved in building critical systems is determined by the standard of the models, methods, tools, techniques and people that are employed during its development. Objective measures of the quality of these resources and methods used in the development of a system can thus provide a useful guide to the level of reliability of the system itself, once developed.

This is largely the approach that was taken by the Commission in reviewing the chosen system. Details of the models, methods, tools, techniques and people that were employed during the development of the chosen system are contained in private documents of the Manufacturers which

[13] (1) Electronic Voting and Counting System: Request for Tenders (Department of the Environment, Heritage and Local Government, 23 June 2000).
(2) Response by successful tenderer to questions in section 4 and appendix F of the Request for Tenders document (Nedap-Powervote, 14 August 2000).
(3) Requirements for Voting Machines for use at Elections in Ireland (DVREC–2, Department of the Environment, Heritage and Local Government, 5 March 2003).

were also provided to the Commission for review.

Verification of Standards

The most obvious way of verifying if a critical system was built following standard practice is to first check the requirements documentation for an explicit statement of the level of reliability that was expected. The absence of such a statement makes it very unlikely that the system was developed accordingly. In the case of the chosen system, many of these requirements were largely pre-determined by the fact that an existing design of electronic voting system was adopted and adapted for use in Ireland and that their existence was thus already implicit or explicit in that design.

Provided that such a requirement of reliability was notified to the developers, the next step is to check that the final system has been tested against that requirement. The absence of such tests makes it unlikely that the system was developed according to its requirements, while the existence of such tests demonstrates only that the developers were trying to build the system following recognised standards, but does not actually guarantee that they have done so.

The final step is to ask systems engineering experts to "look under the bonnet" of the system. Their expertise is likely to be the best tool for assessing the quality of the development process, particularly in cases where other sources of evidence are inadequate, incomplete or absent for one reason or another. It was in this area that much of the Commission's work was concentrated, together with reviewing, as far as possible, evidence of the steps already completed as outlined above.

Requirements and Specifications

One fundamental measure of the quality of any system is how well it meets the purpose for which it was intended. Requirements engineering is concerned with making sure that this purpose is well-understood and that what the customer wants is what the engineers attempt to build. It involves the discovery of purpose by identifying stakeholders and their needs, followed by documenting this in the structured form of a "requirements model" that is amenable to further analysis, communication and subsequent implementation through design.

Analysis

The analysis tools and techniques used in requirements engineering draw upon a variety of domains including computer science, information systems engineering and cognitive and social sciences relative to the context in which the development is taking place. Failure to address any one of these aspects is likely to lead to a system of poor quality.

Effective analysis for building requirements models is also dependent on knowing the sort of information that is required, extracting it, and recording it. There are a number of inherent difficulties in this process. Stakeholders may be numerous and distributed, with differing goals and expectations of the system. In the case of electronic voting, the stakeholders include voters, candidates, electoral authorities, election officials and others. Furthermore, some goals may not be explicit or may be difficult to articulate, and, inevitably, meeting these goals may be constrained by a variety of factors.

Often, as in the case of the adaptation of the chosen system for use in Ireland, an implementation architecture exists such that new requirements must be built onto an already developed system. In this case it is very important that a correct abstraction of the already existing system is incorporated into the requirements model. The requirements also have to be verified to show the logical consistency of the different needs (both old and new) and different points of view. The process of requirements engineering continually improves its models until the best abstraction of the client's needs is reached; and design can begin to transform the *what* into the *how*.

Modelling

Modelling is a fundamental activity in requirements engineering: enterprise modelling, data modelling, behavioural modelling, domain modelling, non-functional requirements modelling, functional requirements modelling, etc., all offer different mechanisms for reasoning about different parts of a system. Good requirements engineers know how to combine these models in order to best capture the needs of the stakeholders.

Once validated, the requirements model should act as a contract between the client and the developer. Subsequently, it should also be possible to verify independently that an implementation is correct with respect to the customer's requirements.

The requirements model is thus important because it acts as the communication medium through which the client, analyst and developers can improve their mutual understanding of the client's requirements. In critical applications it is usual to emphasise the need for client-oriented models: if the client cannot understand the requirements, then validation cannot be done correctly and the rest of the development process is compromised.

Management and Traceability

Requirements management and traceability concerns the ability of developers not only to develop requirements models but also to do so in a form that is readable and traceable by a wide range of readers in order to manage their evolution over time. This has led to the development of a variety of documentation standards that provide guidelines and tools for structuring requirements documents.

Prototyping

When requirements are not well-understood, rapid prototyping can play a role in the iterative extraction and refinement of requirements. A prototype software system is one that simulates the important interfaces and performs the main functions of the intended system, while not necessarily being bound by the same hardware speed, size or cost constraints. Prototypes typically perform the mainline tasks of the application, but make no attempt to handle the exceptional tasks, respond correctly to invalid inputs or abort cleanly. The purpose of the prototype is to make real the conceptual structure specified so that the client can test it for consistency and usability.

However this is not to suggest that the prototype becomes the final system. In fact, there is so much risk involved in this happening (mostly concerned with such a system being impossible to maintain) that software process managers put explicit procedures in place to make sure that a prototype cannot be deployed in this way.

The Commission approached its work, and reviewed the documented requirements of the chosen system, on the basis of this understanding of the importance of requirements engineering in the context of a mission critical system.

Approaches to Systems Verification

It is necessary also to outline at this point the Commission's understanding of how the verification of computer systems may be approached.

There are two fundamental approaches to verification: experimentation and analysis. Experimenting with the behaviour of a system or component to see whether it behaves as required or expected is generally referred to as "testing" and is classified as a dynamic approach. Analysing the product to deduce its correct behaviour or otherwise as a logical consequence of the code resulting from the design decisions is classified as a static approach. Both approaches are founded on the availability of a model of correct behaviour to verify the system against.

Verification by Experimentation (Testing)

Testing exercises a system under representative situations. In general, it is never possible to test system behaviour in all possible situations that might arise, so a suite of test cases can provide only enough evidence to give a degree of confidence that the system is correct, even for cases not tested. Testing can show the presence of errors but, in reasonably complex systems, can never prove their absence. There are also strong theoretical foundations which define procedures for testing that can increase the confidence in tests by exercising the system in such a way that errors are more likely to be found. This theoretical work falls naturally on the boundary of "formal methods" (see below), and the role of requirements and specifications is generally critical.

Verification by Analysis

In many engineering disciplines, analysis complements experimental verification. The goal of analysis is to provide confidence that a system is free from error or is correct with respect to its requirements and specifications. Informal analysis includes code inspections, walkthroughs, etc., and, while these play an important role in increasing the verifiers' confidence in the competency of the programmers, they do not play a direct role in increasing confidence in the correctness of anything other than trivial systems. Confidence in non-trivial systems may be developed by more formal analysis methods designed to formulate proof of the correctness of the code itself. However, there is not widespread competence among software engineers in working with these types of formal methods[14].

[14] Formal methods have been successfully applied in the development of large-scale industrial systems. Their success has largely been due to their integration into the development process from the beginning of the project and throughout every single step of development. In this way, every single design step/decision can be verified and the gap between what is required and what is implemented is spanned by a strong network of interconnected proofs. However, such ideal development conditions are not always present in every situation and, furthermore, formal analysis is somewhat constrained in three fundamental respects: computability, complexity and mathematical competency.

Combined Approaches

Thus, neither experimentation nor analysis is sufficient on its own to verify many real-world systems. In practice, most software engineering projects involve a mix of static and dynamic techniques. However, there are alternative middle ways that are classified as being somewhere between testing and analysis. They are not just a mix but an integration – where the synthesis of the approaches are brought together in a single verification method. One of the most mature accepted approaches is "model checking"[15].

The Commission's Approach

The Commission decided to focus on a pragmatic, technology-oriented approach to its investigation of the chosen system. At the outset it was intended to seek evidence of whether the system met its intended requirements by a formal process of model checking, in combination with testing and informal analysis as appropriate.

A phased and structured programme of work was drawn up in which it was planned that the following phases of activity would be undertaken, with the outcome of each phase informing the Commission's decision to proceed with the next following phase:

- Software Review
  - Review of software architecture, design and development documentation
  - A targeted/focused source code review

- Code Inspection
  - Source code inspection, metrics analysis and coverage indices
  - Unit testing

- Software Testing
  - Testing of the software using sample data approved by the Commission

- System Testing
  - End-to-end testing
  - Parallel testing
  - Other testing as required

Further details of the work envisaged by the Commission are provided in the Commission's Request for Tenders (Computer Software Assurance and System Testing Services)[16] published in November 2004.

[15] Model checking is a pragmatic approach to static analysis. When a system is modelled as a finite state machine, the most relevant or interesting properties can be checked automatically. The separation of functionality - critical from non-critical, and core from non-core - is integral to building an abstract model to be checked. It is an approach which normally requires working with two or more languages – one or more for modelling the system and its operations and a second for asserting the system's properties.

[16] The Commission's request for tenders is available at *www.cev.ie/htm/tenders/software_testing.htm*.

Initial Review

The Commission accordingly engaged the services of persons and bodies having expertise in these areas and the Commission's initial detailed review of the chosen system was carried out on this basis in early 2005. During this phase, the source code, specifications, requirements and associated documentation relating to the design, development and testing of the chosen system were reviewed.

It was decided as a result of this review that the documented requirements and specifications of the system as a whole, and the design and development of the election management software in particular, were insufficiently clear to sustain the Commission's intended formal analysis approach but that it would nonetheless be possible to carry out less formal analysis and testing in order to assess the system further.

On this basis, the Commission refined its approach to the evaluation of the chosen system. In place of the intended proof of the system by modelling, the Commission sought to gather, through analysis and focussed testing of the system, sufficient evidence of its secrecy and accuracy to support a case for its proposed use at elections in Ireland.

Assurance Case

The evidence gathered for this purpose spanned both the hardware and software aspects of the system. This evidence was then arranged in the form of a "structured argument", the highest level argument being that "the system is secret and accurate". In support of this argument, statements such as "the vote recording process is secret", "the vote transmission process is secret", "the vote counting process is secret" needed to be satisfied before the overall argument could be satisfied. Each of these statements in turn needed to be satisfied by further subordinate statements "the voting machine display does not retain the vote once it has been recorded", and so on, until the lowest level of necessary statements was reached, these statements being expressed in terms of specific hardware or software functions of the system such as "the software will always clear the display once a vote has been cast". These lowest level statements then needed to be satisfied by evidence gathered directly from the Commission's work. In this way, the Commission built up an "assurance case" for the secrecy and accuracy of the system based on the evidence of its work.

Although it was intended only to be used at this time for the specific purpose of the Commission's work in examining the secrecy and accuracy of the chosen system, this approach to the assurance of the system, together with the work undertaken to date by the Commission on this basis, could also be used in the future to build up a comprehensive assurance case covering all aspects of electronic voting in Ireland.

Methodology

Expert Assistance

Persons and bodies having specialist expertise in areas including electoral law, information technology and information security were engaged by the Commission to advise and assist it in its work as provided in its terms of reference and in accordance with relevant public procurement procedures.

By competition notices[17] dated 10 November 2004 in the Official Journal of the European Communities and 5 November 2004 and 16 February 2005 in the Irish Government Tendering website, the Commission invited tender proposals for work in the following areas:

- Computer Software Assurance and System Testing Services;
- Review of Hardware Security;
- Review of Physical Security.

The persons and bodies to whom contracts for work were awarded on foot of these competitions carried out their work in accordance with parameters set out by the Commission and subject to its approval, direction and control. The reports of this work were then considered by the Commission.

Project Management

The Commission's own work in connection with the presentation of this report was conducted substantially in accordance with recognised project management standards[18], including as regards quality assurance of the outputs of the work carried out by expert persons and bodies engaged by the Commission.

Privacy and Confidentiality

The Commission considered it necessary and appropriate that its work be carried out in a manner that was free from interruption, influence or interference, and accordingly determined that it would continue to meet and work in private to prepare this report as it had done for the purposes of its earlier reports.

Persons and bodies engaged by the Commission were requested to observe confidentiality in their work and to declare any material interest they may have in the work of the Commission or in the outcome thereof. Except where otherwise indicated, the Commission intends to maintain this confidentiality in respect of matters and materials concerning its work that are not specifically presented in this report.

In addition to the necessary confidentiality and non-disclosure measures implemented by the Commission for the purposes of its work, section 27 of the Electoral (Amendment) Act 2004 also prohibits the disclosure of information relative to the business of the Commission or the performance of its functions and confers absolute privilege on its documents, meetings and reports.

These provisions are necessary to ensure the integrity of the Commission's work and also to protect the intellectual property of the Manufacturers of the chosen system.

[17] These notices can be referenced at http://www.etenders.gov.ie/Authority/Notice_PubView.aspx?ID=NOV030158, http://www.etenders.gov.ie/Authority/Notice_PubView.aspx?ID=FEB033443 and http://www.etenders.gov.ie/Authority/Notice_PubView.aspx?ID=FEB033442.
[18] "PRojects IN Controlled Environments" (PRINCE2), Office of Government Commerce (UK), 1996.

2.4 Overview of the Work

On the basis of the scope and approach to the work outlined above, the Commission's work programme for the purposes of this report included work in the following areas:

- Software Assurance (*Part 3*): Investigation of the quality and reliability of the software, having regard to its defined requirements and specifications, the design and development process, the system documentation and the source code.

- Hardware Security (*Part 3*): Usability analysis and assessment of the security of the hardware components by inspection, modelling and structured analysis methods and in the context of their use at elections in Ireland.

- Testing (*Part 3*): Extension of the Commission's previous testing of the vote counting software from 10,000 to 100,000 sample election test cases; testing of the hardware for susceptibility to hacking, electromagnetic eavesdropping or interference and power supply disruptions.

- Physical Security (*Part 4*): A "life-cycle" review of the physical and operational security arrangements for the design, development, manufacture, transport, storage, deployment and use of the chosen system.

- Comparative Assessment (*Part 5*): Identification and comparative assessment of secrecy and accuracy criteria as between the chosen system and the paper system of voting in Ireland.

- e-Voting Best Practice (*Part 6*): Evaluation of the overall implementation of electronic voting in Ireland with reference to the legal, operational and technical measures contained in the 2004 Council of Europe recommendation on electronic voting.

This work, together with the Commission's findings, conclusions and observations arising from the work is described in more detail in the relevant parts of this report as indicated in each case above.

2.5 Preparatory and Concluding Work

The total elapsed time, from the approval by the Houses of the Oireachtas in June 2004 of the Government's request that the Commission make further reports on the chosen system, to the presentation of this report in July 2006 is 25 months.

Within this timeframe, the actual work necessary to meet the Government's request was carried out in the 10-month period from January to October 2005 in accordance with the Commission's work programme which was cognisant of the possible proposed use of the chosen system at a referendum in November 2005. The Commission was also mindful in this period of the Government's further indication, in June 2005, that the Commission should be asked to complete its work by early 2006 at the latest, although this did not operate as a constraint on the work.

During the periods that preceded and followed the 10-month timeframe of the work outlined above, the Commission was fully engaged in preparatory and concluding activities concerning its work. A significant amount of this effort was directed to overcoming the constraint, identified in the

Commission's earlier reports[19], whereby it had not previously been possible for the Commission to obtain access to the full source code of the chosen system, as well as other intellectual property of the Manufacturers. Moreover, it was necessary for the Commission to ensure that all aspects of its work were undertaken with due care and to a high standard.

Activities undertaken by the Commission in preparation for its work accordingly included the following:

- compliance with public tendering procedures to procure specialist services;
- negotiation of contract terms and detailed work to be carried out by contractors;
- negotiation of non-disclosure terms with Manufacturers and contractors;
- provision of indemnities by Government in respect of non-disclosure liabilities;
- implementation of security measures to underpin non-disclosure and indemnity terms;
- confirmation by the Department of a "stable version" of the system on which to base the Commission's work;
- provision of confidential materials by the Manufacturers to contractors for review.

Activities undertaken by the Commission following the conclusion of its work included:

- quality review, clarification and refinement of work carried out by contractors;
- report drafting and review;
- consultation on draft report with Manufacturers, Department and others.

The Commission believes that this necessary and important additional work has contributed substantially to the integrity of its overall work in a way that can, in turn, contribute positively to the future development of electronic voting in Ireland.

2.6 Consultation

Following completion of the Commission's work, the Manufacturers and the Department were invited to review and comment on the Commission's draft report. Where it was found appropriate or necessary, their observations on specific points have been accepted by the Commission and are incorporated in this report. Any other observations on specific points that were not accepted by the Commission or that did not require to be accommodated (being by way of commentary, additional information or clarification only) have been included at *Appendix 7* to this report.

[19] First Report of the Commission on Electronic Voting, December, 2004: Part 2 p.31.

2.7 Electronic Voting Context

This section outlines where the Commission's work lies in the context of electronic voting generally.

Electronic Voting Developments

The Commission recognises that its work has taken place at a time of significant "climate change" with regard to electronic voting generally. During this time, voting technologies have been required to meet and adapt to new challenges that have arisen as a result of significant alterations in the levels of public and political expectation and acceptance of electronic voting, both in Ireland and abroad.

In the United States for example, where the use of electronic voting is becoming increasingly widespread[20], significant concerns surrounding the integrity of voting equipment and electoral processes have led to the enactment of measures specifically targeted at the regulation of electronic voting, including through the provision of paper audit trails as a mandatory requirement.

Within Europe, where electronic voting is also becoming more widespread, there are clear signs of movement towards a common standard on electronic voting with the adoption in 2004 of a Council of Europe recommendation[21] on legal, technical and operational aspects of electronic voting.

Consideration of these "climate change" issues lies mainly outside the scope of the Commission's work as currently framed by its terms of reference but they do raise the significant question for the Commission of what standards it should apply to its consideration of the system. If, for example, the Commission were engaged in a review of the decision to adopt the chosen system, then the appropriate standards would be those which applied at the time of its procurement, while the standards against which the system is tested and evaluated prior to its use at real elections must be the standards of today.

While recognising that there will always be a difficulty in measuring any particular electronic voting system against the moving targets of public expectations and advancing technology, the particular standards adopted by the Commission within the narrower scope of its own terms of reference in relation to the secrecy and accuracy of the chosen system are described in *section 2.2*.

Electronic Voting in Ireland

Based on these wider developments and on the perceived and reported conclusions of the Commission's previous reports and the subsequent non-use of the chosen system, the Commission also recognises that the public perception of the current and future status of electronic voting in Ireland may differ from what the Commission was able to consider in its work and in making its reports.

[20] Source: US Election Data Services Voting Equipment Study 2006: www.electiondataservices.com.
[21] Recommendation Rec(2004)11 of the Committee of Ministers of the Council of Europe.

In particular, consideration of the practical, administrative, political and other requirements that formed the basis of the adoption and procurement of the chosen system for use in Ireland lies largely beyond the scope of the Commission's work, as do some of the more general e-voting objectives on which opposition to the system in Ireland has been based.

While the Commission's work has thus been more narrowly focussed than might generally be perceived or expected, the relevant issues of secrecy, accuracy and testing of the chosen system are nonetheless broad in their application and are essential attributes of any voting system, when viewed in a broader context. For this reason, the exclusion of the various matters referred to above has not acted as a limitation on the Commission's work.

The Commission has also endeavoured, within the particular context of its terms of reference in relation to secrecy and accuracy, to shed as much light as possible on the chosen system, given the natural tension that exists between the proprietary nature of many of its components and the fundamental requirement that electronic voting systems must offer the highest levels of transparency, accountability and demonstrable reliability if voters are to have confidence in them.

In this way, by reporting to the fullest possible extent on the general nature of the chosen system, its specific characteristics and the operational arrangements for its deployment, the Commission believes that its work can contribute to greater public knowledge and understanding of the chosen system.

Consistent with its independent role, the Commission has maintained an open view on electronic voting in general, while acknowledging that its introduction in Ireland can make a positive contribution to inclusive and representative democracy. There are clear benefits and advantages associated with electronic voting and, although consideration of some of them lies beyond the scope of the Commission's work, many of these benefits and advantages are represented in the chosen system.

Within the particular scope of its terms of reference, the Commission also recognises that, when compared with paper voting, electronic voting methods in general can deliver enhanced levels of accuracy and similar levels of secrecy and that this potential also exists in the particular case of the chosen system.