

# Electronic Voting: A Safety Critical System

Margaret Anne McGaley

Final Year Project - 2003  
March 4, 2003  
B.Sc. Computer Science and Software Engineering



NUI MAYNOOTH

Oilscoll na hÉireann M<sup>A</sup> Nuad

Department of Computer Science,  
National University of Ireland, Maynooth  
Co. Kildare  
Ireland

A thesis submitted in partial fulfillment of the requirements for the B.Sc. Computer Science and  
Software Engineering.

Supervisor: Dr. J. Paul Gibson

## Declaration

I hereby certify that this material, which I now submit for assessment on the program of study leading to the award of B.Sc. Computer Science and Software Engineering, is entirely my own work and has not been taken from the work of others - save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: ..... Date: .....

### **Abstract**

This project was motivated by the growing apprehension among Irish citizens over the electronic voting system being introduced here. The aims of the project were three: to discover what would be required of an electronic voting system to make it a suitable replacement for the existing paper-ballot system; to examine whether the Nedap/Powervote system meets those requirements; to begin the process of designing and implementing a system which could meet the requirements. The first two goals were achieved through research into the opinions of experts on electronic voting and computer security. The third was achieved with the use of formal methods.

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Aims and Motivation . . . . .	4
1.2	Electronic Voting . . . . .	4
1.3	Formal Methods . . . . .	5
1.4	Overview of the Report . . . . .	6
<b>2</b>	<b>Tools and Skills Learned</b>	<b>7</b>
2.1	Research . . . . .	7
2.2	L <sup>A</sup> T <sub>E</sub> X . . . . .	8
2.3	CafeOBJ . . . . .	8
<b>3</b>	<b>Results</b>	<b>9</b>
3.1	Electronic Voting . . . . .	9
3.2	Proposed Modifications and Their Implications . . . . .	10
3.3	Specifications . . . . .	11
3.3.1	Development . . . . .	11
3.3.2	Verification of Safety . . . . .	11
3.3.3	Addressing Incompleteness – A Validation Issue . . . . .	12
3.3.4	Testing . . . . .	13
<b>4</b>	<b>Discussion</b>	<b>14</b>
4.1	Summary of Work Done . . . . .	14
4.1.1	Research . . . . .	14
4.1.2	Formal Specification . . . . .	15
4.2	Proposals for Enhancement . . . . .	15
4.3	Critical Appraisal . . . . .	15
	<b>Bibliography</b>	<b>16</b>
<b>A</b>	<b>: Electronic Voting Systems Currently Available</b>	<b>20</b>

<b>B : Proportional Representation - Single Transferrable Vote</b>	<b>21</b>
<b>C : Interim Progress Reports</b>	<b>27</b>
<b>D : Specifications, Implementations and Tests</b>	<b>30</b>
<b>E : Research Report</b>	<b>32</b>

Note: This document should be read in conjunction with *Electronic Voting: A Safety Critical System. Research Report, NUI Maynooth Department of Computer Science 2003* also by Margaret McGaley (see appendix E).

## Acknowledgements

Thanks to God, for everything.

Thanks to my family for their love.

Thanks to Paul Gibson, for all his hard work.

Thanks to my friends

Cian, Kevin and Claire

for their love, support and interest

... and their coffee.

# Chapter 1

## Introduction

### 1.1 Aims and Motivation

The aims of this project were: to investigate the current state of the art with regard to electronic voting systems (EVS); to develop a set of requirements for an acceptable EVS; and to begin the production of such a system by formally specifying and implementing the most complex of its components – the count software.

The introduction of the Nedap/Powervote [1] system for kiosk voting in Ireland provoked interest in the subject within the Irish computer science community. Complaints that the the system is insecure have been dismissed as paranoia [2]. The authors wanted to show that complaints were not the result of paranoia and that the Nedap/Powervote system was not an acceptable replacement for our paper-ballot system.

### 1.2 Electronic Voting

Electronic voting is any form of vote collection involving electronic (usually computer) devices. The method by which votes are collected is fundamental to democracy. Any vote collection system that could be manipulated to affect the outcome of elections, could potentially pose a threat to people's lives in the country where it was in use. Therefore electronic voting systems can be considered safety critical [3].

## 1.3 Formal Methods

In a safety critical system, where correctness is vital, it is infeasible to rely on testing. The number of tests needed to prove correctness within required limits can be astronomical [4].

Formal methods offer us a development strategy which can significantly reduce the number of errors in our final system. According to Holloway [5], the most rigorous method of software development available today is the use of Formal Methods. Possibly the most famous example of their successful use is the driverless line 14 of the Paris metro [6].

Formal specification gives us the power to clearly express our meaning, across natural language barriers. Just as legal language was developed to prevent misinterpretation of law, formal specification was developed to prevent misinterpretation of specifications [7]. This unambiguity means that formal specifications can easily be automatically processed by software, unlike natural language. Formal specifications can be automatically checked for ambiguity, incompleteness, and contradiction. They can also be refined in stages from abstract to concrete specifications.

While programming languages are formal enough to be automatically processed, they force the author to think about how functionality can be produced. Formal specifications allow the author to specify what the desired behaviour is first, before considering implementation. Many software faults arise at the design stage because of conflicting or misunderstood requirements. The use of formal methods can highlight these mistakes at a stage where they are more easily spotted and rectified. Once the specification is correct and complete, the final product can be produced in automatic and semi-automatic stages.

Formal methods are less widely used than their proponents would like. The specifications can seem cryptic to the uninitiated, and the mathematics involved puts many people off. There is a perception that formal methods do not involve the same creativity as programming. But as Mr. Andrew Harry says:

“There are as many ways of writing a formal specification as there are of programming it. Needless to say, only a few of these ways are good.” [7]

Despite their “public relations” difficulties, formal methods are indispensable in the development of safety critical systems, where correctness is of the utmost priority.

The authors have not found any EVS developed using formal methods.

## 1.4 Overview of the Report

This final year project report is considerably shorter than average. This is mainly due to the fact that the project did not focus on the development of a software product. Its aims were the investigation of electronic voting, and taking the first steps towards the development of an EVS. As such, there was no software design process in the usual sense of that phrase, and the specifications are themselves the code.

In this chapter we introduced the project, electronic voting and formal methods. We go on, in chapter 2, to describe the tools used and the skills learned during the project. Chapter 3 discusses our results regarding electronic voting, the modifications proposed and the development and testing of specifications. Finally, in chapter 4, the project is reviewed and appraised.

Four appendices are included. The first lists the EVSs found during the research phase. The second contains flowcharts representing Proportional Representation - Single Transferrable Vote (PR-STV), the process of counting used in Irish elections. The third gives the interim progress reports for this project. The last contains web references to the specifications and support software developed.

## Chapter 2

# Tools and Skills Learned

### 2.1 Research

This project involved deeper research than the student author has ever had to do before. It was necessary to gather information, filter it for usefulness and relate it succinctly in the research report [8] accompanying this document.

Being a relatively young field, the published literature on electronic voting is sparse. As a result, much of our investigation relied on the considerable resources available on the Internet.

The single most valuable resource on the World Wide Web is the webpage of Dr. Rebecca Mercuri [9]. There were some published articles about the subject, including two particularly useful ones in *The Communications of the ACM* [10, 11]. Three books found useful while researching the history and philosophy of voting were: Peter Singer's "Democracy and Disobedience" [12]; Cornelius O'Leary's "Irish elections, 1918-77 : parties, voters, and proportional representation" [13] and Cynthia Farrar's "The Origins of Democratic Thinking - The invention of politics in classical Athens" [14]. In researching Formal Methods, Andrew Harry's "Formal Methods Fact File : VDM and Z" [7] was found particularly useful.

Apart from seeking information in books and on the web, contact was made with the Department of Environment and Local Government (DoELG). Some information which was not readily available, including the report from Zerflow [15], was requested and received under the Freedom of Information Act [16]. Mr. William Stapleton of the franchise section was very helpful in our correspondence.

## 2.2 L<sup>A</sup>T<sub>E</sub>X

L<sup>A</sup>T<sub>E</sub>X [17] is a macro package, which runs on the T<sub>E</sub>X [18] program. It is a very powerful typesetting program, generally used for formatting large documents. T<sub>E</sub>X itself is actually more powerful, but the macros in L<sup>A</sup>T<sub>E</sub>X make it much more accessible. In contrast to “what you see is what you get” (WYSIWYG) word processors, L<sup>A</sup>T<sub>E</sub>X files are created as plain text files, containing commands which are interpreted when the L<sup>A</sup>T<sub>E</sub>X program is run. The output is a Device Independent (.dvi) file which can then be converted into many different file formats.

L<sup>A</sup>T<sub>E</sub>X has a higher learning curve than its WYSIWYG competitors, but it has several advantages over them.

Very large documents are possible with L<sup>A</sup>T<sub>E</sub>X, because the originals are edited in a simple text editor. It is frequently used for typesetting books, something which would be impossible with the better known word-processors.

It is much easier to have a clear style when using L<sup>A</sup>T<sub>E</sub>X. The style is set at the beginning of the document, and determines how later commands are interpreted. For instance, the size of chapter headings and the format of quotations for the whole document can be determined at the beginning. This results in a clear consistent style.

Similarly, if for some reason the author wishes to change the style of their document, this can often be done by changing just one line within the original plain text file.

The table of contents and bibliography (among other things) can be automatically generated, saving the author time, and preventing inconsistencies.

## 2.3 CafeOBJ

CafeOBJ, available on the web at [19], was used to develop the formal specifications. It is an algebraic specification and programming language, a direct successor of OBJ [20]. The interpreter runs on Common Lisp [21].

CafeOBJ was chosen over other languages for several reasons. It is free, it has good tool support, it is good for working at the requirements and design levels of abstraction, it maps well onto an Object Oriented implementation and it was considered suitable for proving properties of the underlying e-voting systems specified. Other languages considered were LOTOS [22] and B [23].

# Chapter 3

## Results

### 3.1 Electronic Voting

There are four main advantages that an EVS could potentially provide: A faster count; a more accurate count; increased fairness within PR-STV; and expanding the franchise [8]. However, whatever advantages it offers, electronic voting should only be introduced if it does not increase the danger of election manipulation.

It must be possible to independently reproduce the results generated by the EVS, and because of the nature of computer systems this requires a paper vote trail. The voter's privacy must be safeguarded, which rules out remote electronic voting (for example over the Internet). If it is to be worth using the electronic system at all, then it must always produce the correct result – which can then be verified when necessary by counting the paper ballots. It must, therefore, be developed using formal methods. It is also reasonable for the Irish public to demand that the software source code of the system be made publicly available – that the system be made “open source”. Claims that this would be a threat to the security of the system [24] are unfounded. It would, in fact, increase the security of the system. According to Mr. Bruce Schneier – computer security expert and cryptographer:

“In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.”  
[25]

Faults, accidental or otherwise, are much more likely to be detected if many people are viewing the source code than if it was only reviewed once by a small number of developers in a private company. The source code for the EVS recently introduced in Australia is publicly available on the web [26].

Almost all of the systems found during our investigation were commercial applications (see appendix A). None of them were developed using formal methods. As is standard practise in commercial software development, these applications are closed-source. Given the complexity of these systems, it is likely that they contain vulnerabilities and errors, particularly since they were not developed formally.

This project focuses on the Nedap/Powervote system bought by the Irish government. As a result of our investigation [8] we have concluded that this system is not an adequate replacement for our paper-ballot system. It was not developed formally, its source code is not freely available, and it does not provide a paper audit trail.

The research report [8] which accompanies this document explains all of these findings in greater detail. It also highlights certain properties of the system which we believe point to a lack of rigour in its development.

## 3.2 Proposed Modifications and Their Implications

We propose the development and introduction of an entirely new system, developed by Irish nationals. The source code for both the voting booth and the count software would be available to the public for inspection, as is the case for the Australian system [26]. In the research report for this project [8] we also specified other aspects of our ideal voting system, including: the use of formal methods in its development; and the printing of a ballot paper for each vote – the Mercuri Method [27].

The first major implication of this project is that the Nedap/Powervote system should never have been used in national polls, and certainly should not be introduced nationwide. The second implication is that it may not be worthwhile for Ireland to introduce electronic voting at all.

The development and running of the system we propose is unlikely to cost less than the existing paper system, especially since the same number of ballot papers would be used. Also, the government have estimated that the Nedap/Powervote system will cost them 32 million euro [28]. Presumably this money could not be recouped if the government did decide not to introduce

the system at this late stage. The advantages which an EVS could potentially provide are possibly not significant enough in a country the size of Ireland to warrant spending more.

### 3.3 Specifications

All the code developed – in CafeOBJ, Java and Perl – is available on the web. Please see appendix D for details.

#### 3.3.1 Development

The election rules for PR-STV are defined in the third schedule of the Electoral Act, 1923 [29]. This document provides the most formal definition of the PR-STV count process found during our investigation. It is not formal enough for our purposes, however. To aid in understanding of the count process, flowcharts were developed (see appendix B). These informal requirements were then developed into formal specifications in CafeOBJ.

#### 3.3.2 Verification of Safety

One of the advantages of using formal methods is that we can check safety properties of the system being developed. An example of this in the case of our EVS is the property that all voters in a constituency must vote from the same list of candidates. This was expressed in the CafeOBJ specifications as a boolean operator called *invariant*:

```
--> eq invariant
    eq invariant(emptyVs(numCs)) = true .

--> ceq invariant
    ceq invariant(addV(Vs,v)) = false
        if ( not( ( numCandidates(Vs)) == (numCandidates(v)) and
                    invariant(Vs) ) ) .

    ceq invariant(addV(Vs,v)) = true
        if ( ( (numCandidates(Vs)) == (numCandidates(v)) and
                invariant(Vs) ) ) .
```

The addition of votes using the *add* operator, which does not perform any checks on the vote added, or the list to which it is added, was proven to be unsafe. That is, a list of votes which met the invariant property before the *add*

operation was performed on it, did not necessarily meet that invariant after the operation. It was, therefore, necessary to add a safe addition operator *addVSafeButWrong* (so named because of its incompleteness, see below):

```
--> ceq addVSafeButWrong
      ceq addVSafeButWrong(Vs,v) = addV(Vs,v)
                                     if ( invariant(addV(Vs,v)) and
                                           invariant(v) and
                                           invariant(Vs)   ) .

      ceq addVSafeButWrong(Vs,v) = Vs
                                     if not ( invariant(addV(Vs,v)) and
                                              invariant(v) and
                                              invariant(Vs)   ) .
```

It was then possible to automatically ‘prove’ that the invariant is respected when this safe addition was done, using the consistency checker in the CafeOBJ tool.

The complete specification (see appendix D) has details of other safety properties checked in a similar fashion.

### 3.3.3 Addressing Incompleteness – A Validation Issue

The formal model is not only useful for addressing inconsistency within specifications; it can also help address the serious issue of incompleteness. To illustrate this point, let us examine ‘spoiled votes’ within our specification.

The legal definition of the PR-STV count process does not explicitly allow spoiled votes, but many people feel that an EVS should provide this facility [30], which exists in the paper system.

The operator *addVSafeButWrong*, as specified in section 3.3.2, does not allow spoiled votes to be added to the system. In this context, a spoiled vote is one whose invariant, or safety property, is false. We therefore need to weaken the safety operator to allow spoiled votes, while ensuring that it is strong enough to continue to check for consistency between votes.

The operator developed for this purpose was *addVSafe*:

```

--> ceq addVSafe
    ceq addVSafe(Vs,v) = addV(Vs,v) if (invariant(addV(Vs,v)) and
                                        invariant(Vs) ) .
    ceq addVSafe(Vs,v) = Vs if not(invariant(addV(Vs,v))and
                                    invariant(Vs) ) .

```

The complete specification (see appendix D) has details of other incompleteness issues that were (or could be) addressed in a similar fashion.

### 3.3.4 Testing

Tests, in the formal model, can be thought of as integral to the validation process. Tests are used to animate/simulate behaviour. CafeOBJ provides executable semantics which can be considered as prototypes. Java and Perl code was developed to automatically produce test cases. Please see appendix D for details about this test code.

Java implementations of the specifications were developed, details of which can be found in appendix D; unfortunately, due to limited time, it was not possible to implement all of the functionality envisaged. It was hoped that the class VoteIO would be capable of reading in the files it produced, and creating Vote and Votes objects representing the same lists of votes. A small recursive-descent compiler that handled the subset of CafeOBJ used in these files would be sufficient.

# Chapter 4

## Discussion

### 4.1 Summary of Work Done

#### 4.1.1 Research

The first phase of the project was research. There were several areas that required considerable research and reading. The main topics were the following: the Irish electoral process; democracy in general; the current state of the art in electronic voting; the opinions of experts in the field.

In the many books published about democracy, and specifically democracy in Ireland, no clear description of the count process used in our elections was found. Eventually the legal definition [29] was used to develop flowcharts representing the process. These flowcharts are included in appendix B. The counting of votes was also the component chosen for formal specification and implementation (see below).

The introduction of an EVS in Ireland could potentially have a serious effect on our democracy. As such, a good deal of the research report which accompanies this paper [8] was devoted to the historical and philosophical context of electronic voting.

During the research into existing EVSs, emphasis was placed on the Nedap/Powervote system, but several other systems (listed in appendix A) were examined.

Several scientists' resources on the web were invaluable to my research, particularly with regard to the requirements we ought to set for an EVS in Ireland. They included Dr. Rebecca Mercuri [9], Bruce Schneier [31] and Douglas Jones [32].

### 4.1.2 Formal Specification

The second phase was the development of formal specifications to describe software which performed the tabulation of votes according to the rules of PR-STV. These were developed in CafeOBJ, with support software written in Java and Perl. The specifications were implemented in Java.

## 4.2 Proposals for Enhancement

Due to limited time, only one component of the voting system was formally specified. Other components, such as the recording of individual votes, and the recording of constituency details could also be formalised.

The interface was not examined in great detail. Aspects worth investigation would be: the opinions of Irish voters as to the preferred behaviour of the system; accessibility for voters with special needs; and the psychology of user interface design.

It would be of great interest to perform a large independent survey of the opinions, both of ordinary voters, and of those heavily involved in the election process. Questions could cover the respondent's feelings on the following topics: is the introduction of electronic voting inevitable; is electronic voting a good or a bad thing; was Nedap/Powervote the right choice; was the selection process carried out in an acceptable manner?

It would have been interesting to examine political philosophy, and electronic voting's place in that complex field, more deeply.

An area worth investigation is the theoretical possibility of a remote authentication protocol which could meet both the authentication requirement, and the privacy requirement. Current security models are incapable of overcoming the intuitive conflict between these requirements.

## 4.3 Critical Appraisal

The research report which was written as part of this project gives a good overview of electronic voting. It involved deep research, and the student author is now well-versed in the complexities of the topic.

The authors had hoped to develop formal specifications for more than one component of the system. The research phase of the project took longer than expected, however, leaving less time for formal specification. It would have been better to finish the research phase and begin the development of specifications in parallel.

The flowcharts representing the PR-STV count process were originally drawn in a trial version of SmartDraw. Unfortunately, this trial version has some very annoying behaviour which makes it impractical for general use. It was necessary to redraw the flowcharts using Microsoft PowerPoint, so that they could be included with this document. If the authors could begin the project again, SmartDraw would not be used.

The single biggest problem within the project was time management. As is common with large projects, deadlines were missed and put back.

Overall the project is a good one. This is an important issue which has not received enough attention from the general public or the computer science community. By highlighting the potential dangers of electronic voting, this project may have a part to play in changing our democracy for the better. It is innovative, in that no formal specification of the PR-STV count system used in Irish elections has been developed before. Even the legal definition is somewhat informal – using phrases such as “and so on” [29]. The extensive research has paved the way for further development of an adequate electronic voting system for use in Ireland.

# Bibliography

- [1] Homepage of the Nedap/Powervote Electronic Voting System.  
*[http://www.election.nl/bizx\\_html/IVS-GB/](http://www.election.nl/bizx_html/IVS-GB/)*.
- [2] Dan White. The real price of electronic voting. *Irish Computer*, 26(10), November 2002.
- [3] Definition of ‘safety-critical system’.  
*<http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?safety-critical%20system>*.
- [4] Why is [sic] Formal Methods Necessary?  
*<http://shemesh.larc.nasa.gov/fm/fm-why.html>*.
- [5] C. Michael Holloway. Why Engineers Should Consider Formal Methods. In *1997 AIAA/IEEE 16th Digital Avionics Systems Conference*, 1997.
- [6] P. DESFORGES. Interlocking System Experience & Prospects. In *FMERail Workshop on Formal Methods in Railway Systems, FM’99 World Congress on Formal Methods, Toulouse, France, 1999*.
- [7] Andrew Harry. *Formal Methods Fact File : VDM and Z*. Wiley, 1996.
- [8] Margaret McGaley. Electronic Voting: A Safety Critical System. Research Report, NUI Maynooth Department of Computer Science 2003.
- [9] Dr. Rebecca Mercuri’s website on electronic voting.  
*<http://www.notablessoftware.com/evote.html>*.
- [10] Aviel D. Rubin. Security Considerations for Remote Electronic Voting. *Communications of the ACM*, 45(12), December 2002.
- [11] Dr. Rebecca Mercuri. Florida 2002: Sluggish Systems, Vanishing Votes. *Communications of the ACM*, 45(11), November 2002.
- [12] Peter Singer. *Democracy and Disobedience*. Gregg Revivals, 1973.

- [13] Cornelius O’Leary. *Irish elections, 1918-77 : parties, voters, and proportional representation*. Gill and Macmillan, 1979.
- [14] Cynthia Farrar. *The Origins of Democratic Thinking - The invention of politics in classical Athens*. Cambridge University Press, 1988.
- [15] Zerflow homepage. <http://www.zerflow.com/>.
- [16] Freedom of Information Act, 1997. Available online at the website of the office of the Attorney General [http://www.irishstatutebook.ie/1997\\_13.html](http://www.irishstatutebook.ie/1997_13.html).
- [17] LaTeX homepage. <http://www.latex-project.org/>.
- [18] TeX Resources on the Web. <http://www.tug.org/interest.html>.
- [19] CafeOBJ Official Homepage.  
<http://www.ldr.jaist.ac.jp/cafeobj/index.html>.
- [20] The OBJ Family homepage.  
<http://www.cse.ucsd.edu/users/goguen/sys/obj.html>.
- [21] Common Lisp. <http://www.apl.jhu.edu/~hall/lisp.html>.
- [22] World-wide Environment for Learning LOTOS (WELL).  
<http://www.cs.stir.ac.uk/kjt/research/well/>.
- [23] J.-R. Abrial. *The B-Book: Assigning Programs to Meanings*. Cambridge University Press, 1996.
- [24] J.D. Michael Ian Shamos, Ph.D. Electronic Voting - Evaluating the Threat.  
<http://www.cpsr.org/conferences/cfp93/shamos.html>, 1993.
- [25] Bruce Schneier. Open Source and Security.  
<http://www.counterpane.com/crypto-gram-9909.html>.
- [26] Electronic voting Technical description of how it works.  
<http://www.elections.act.gov.au/EVACS.html>, 2001.
- [27] Dr. Rebecca Mercuri. A Better Ballot Box? *IEEE Spectrum Online*, October 2002.
- [28] Making it Easier to Vote - Electronic Voting and Counting.  
[http://www.environ.ie/elevote\\_detail.pdf](http://www.environ.ie/elevote_detail.pdf).
- [29] Electoral Act, 1923. Available online at the website of the office of the Attorney General [http://www.irishstatutebook.ie/1923\\_12.html](http://www.irishstatutebook.ie/1923_12.html).

- [30] Breda O'Brien. Electronic voting takes 'craic' out of the count. *The Irish Times*, Saturday, April 20th 2002.
- [31] Bruce Schneier. Counterpane Internet Security.  
<http://www.counterpane.com/>.
- [32] Douglas W. Jones. Voting and Elections.  
<http://www.cs.uiowa.edu/~jones/voting/>.

## Appendix A

# Electronic Voting Systems

Companies in bold were considered for introduction in Ireland. Nedap/Powervote (underlined) was chosen.

Danaher Controls	<a href="http://www.guardianvoting.com">http://www.guardianvoting.com</a>
Diversified Dynamics Inc	<a href="http://www.divdyn.com">http://www.divdyn.com</a>
DZine	<a href="http://www.dzine.be/">http://www.dzine.be/</a>
<b>Election Systems and Software</b>	<a href="http://www.essvote.com/">http://www.essvote.com/</a>
Evote	<a href="http://www.instore.gr/evote">http://www.instore.gr/evote</a>
Fidlar Doubleday Inc	<a href="http://www.fidlar.com">http://www.fidlar.com</a>
Global Election Systems Inc	<a href="http://www.gesn.com">http://www.gesn.com</a>
Hart InterCivic	<a href="http://www.hartic.com">http://www.hartic.com</a>
<b>Indra</b>	<a href="http://www.indra.es/ingles/home.htm">http://www.indra.es/ingles/home.htm</a>
Microvote	<a href="http://www.microvote.com">http://www.microvote.com</a>
<u><b>Nedap/Powervote</b></u>	<a href="http://www.election.nl/bizx.html/IVS-GB/">http://www.election.nl/bizx.html/IVS-GB/</a>
Safevote	<a href="http://www.safevote.com">http://www.safevote.com</a>
Scytl	<a href="http://www.scytl.com/voting.html">http://www.scytl.com/voting.html</a>
<b>Sequoia</b>	<a href="http://www.sequoiavote.com/homePage.php">http://www.sequoiavote.com/homePage.php</a>
Shoup Voting Solutions	<a href="http://www.shoupvote.com">http://www.shoupvote.com</a>
Surveys International	<a href="http://www.surveys-intl.com">http://www.surveys-intl.com</a>
TrueBallot	<a href="http://www.trueballot.com">http://www.trueballot.com</a>
<b>UniLect</b>	<a href="http://www.unilect.com/">http://www.unilect.com/</a>
VoteHere	<a href="http://www.votehere.net">http://www.votehere.net</a>
WebVote Inc	<a href="http://www.webvote.net">http://www.webvote.net</a>
Worldwide Election Systems	<a href="http://www.worldwideelection.com">http://www.worldwideelection.com</a>

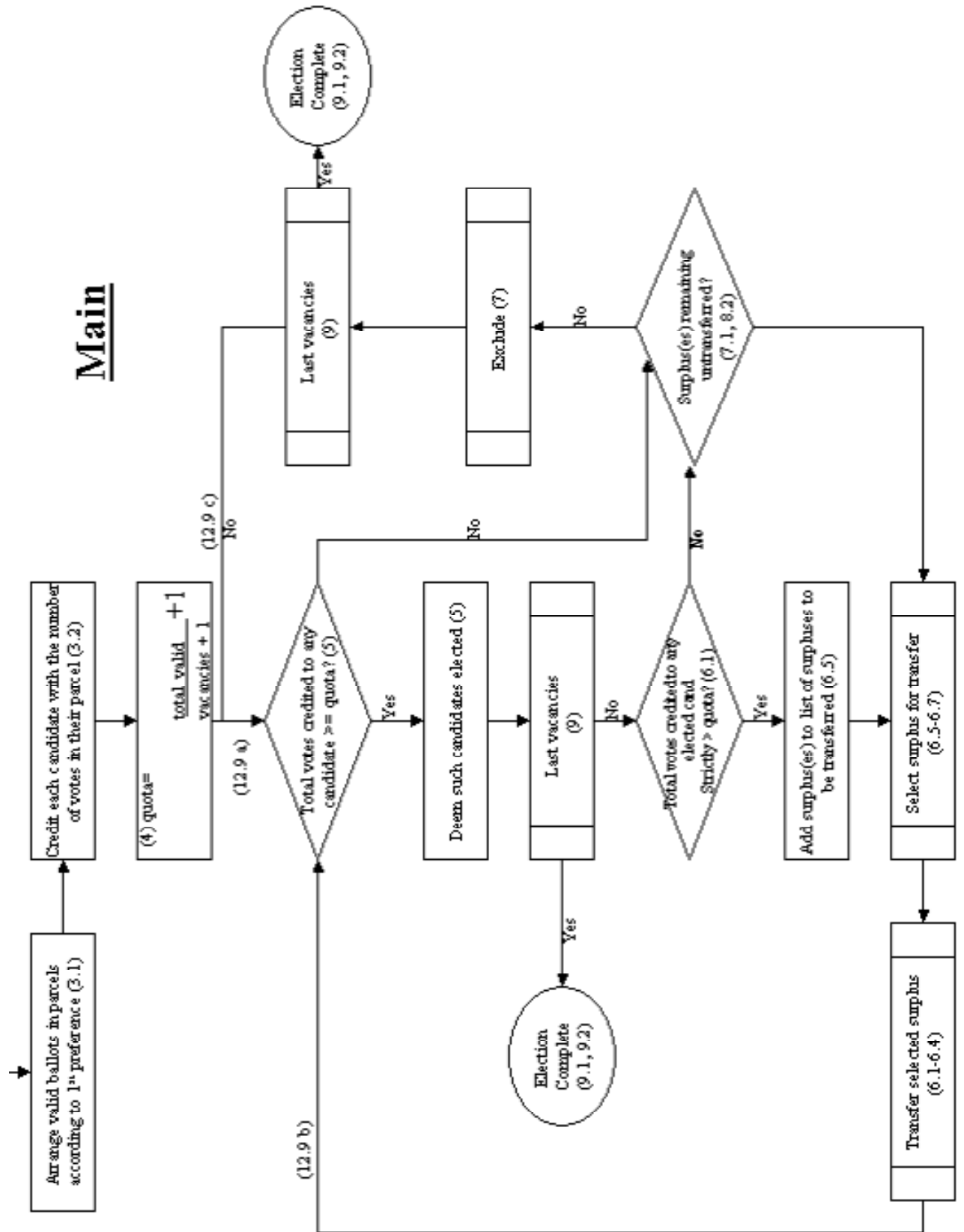
## Appendix B

# Proportional Representation - Single Transferrable Vote

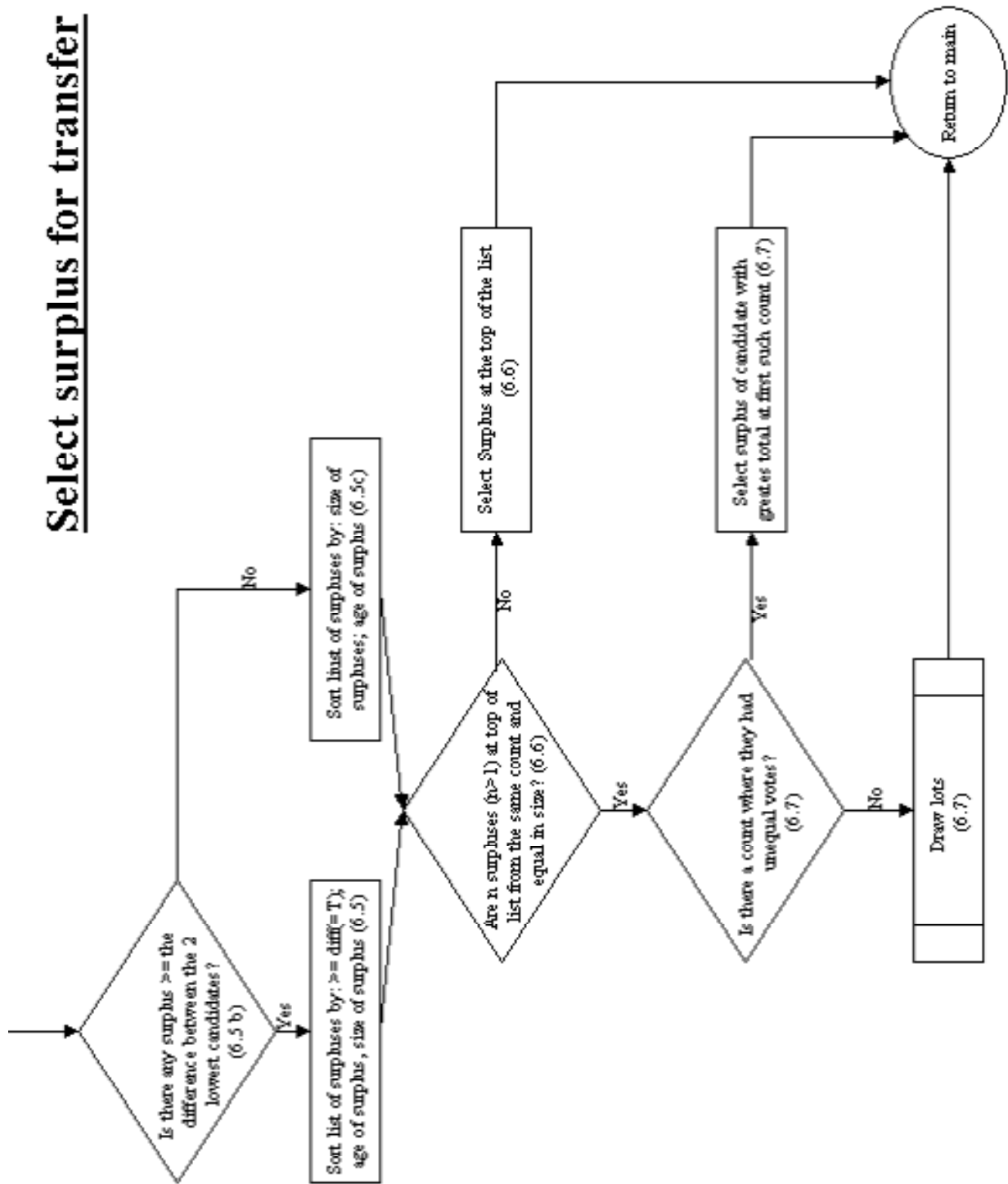
The flowcharts begin on the next page. The first chart, called main, is where execution begins. The numbers within the charts refer to articles in the legal definition of PR-STV, available online at:

<http://www.irishstatutebook.ie/gen131923a.html>

# Main



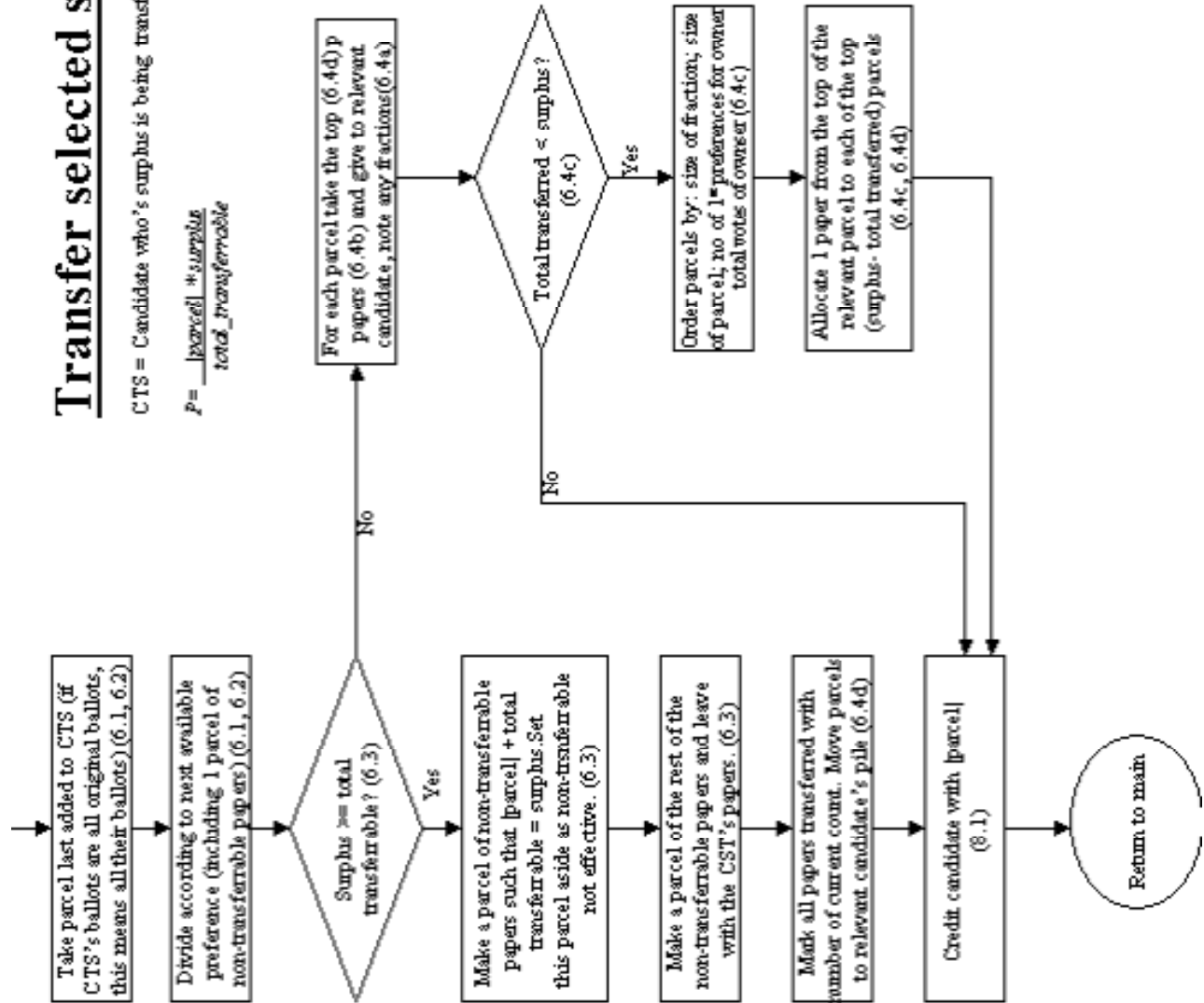
## Select surplus for transfer



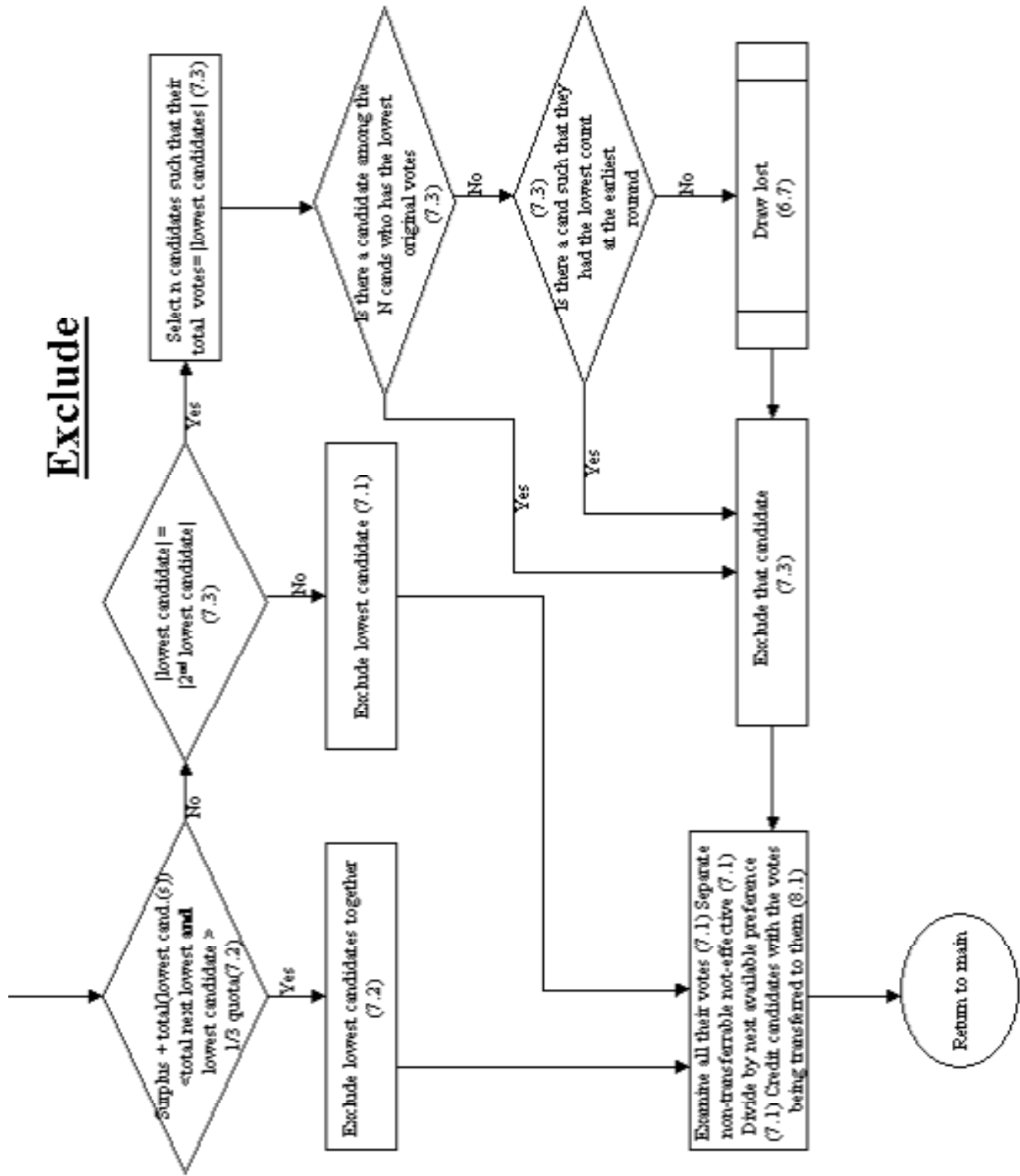
# Transfer selected surplus

CTS = Candidate who's surplus is being transferred.

$$P = \frac{|parcel| * surplus}{total\_transferable}$$

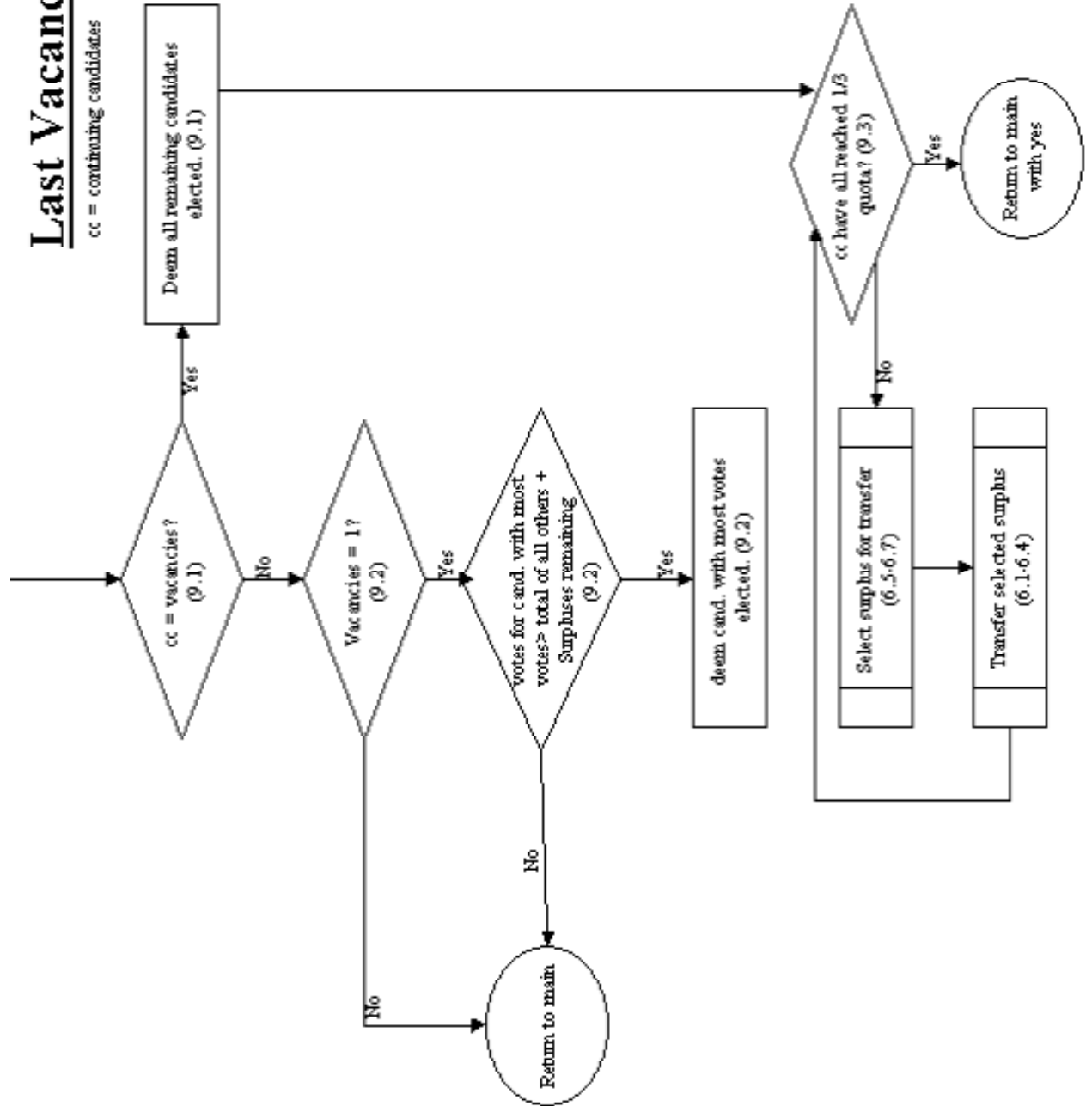


# Exclude



# Last Vacancies

cc = continuing candidates



## Appendix C

# Interim Progress Reports

### Friday 1st of November

There is little to report, because the project is still taking shape. It looks like there is going to be a long research phase in the beginning. I have been reading the LOTOS manual available at

<http://www.cs.stir.ac.uk/~kjt/research/lotos-stir.html>

The formal specifications will probably be written in LOTOS. I have set up a website at

<http://www.redbrick.dcu.ie/~afrodite/Project>

where I will provide links to sites I have found useful in my research. The website of Dr. Rebecca Mercuri

<http://www.notablessoftware.com/evote.html>

looks like it will be very useful. The marking scheme for the project has been agreed.

### Friday 29th of November

We have agreed that the formal specifications will be written in professional B tools if we can get them free of charge, otherwise they will be written in LOTOS/ActOne. I have written an e-mail to Mr. William Stapleton in the Department of the Environment and Local Government (DoELG), requesting information about the Nedap/Powervote system. I have spent a considerable amount of time trying to find an adequately formal description of the Proportional Representation - Single Transferrable Vote (PR-STV) count system. I have borrowed several books from the library, but have been unsuccessful so

far. The document “Direct Vote Recording/Electronic Vote Counting System – Information Paper” dated March 2002 includes flowcharts which supposedly describe count module within the Nedap system. Unfortunately they are incomplete, and contain unexplained references to “channels”. I have been updating my website regularly.

## **Friday 20th of December**

We have agreed that I should concentrate on the research report for the project until after Christmas. I have been reading extensively, looking for people’s opinions on electronic voting, and for formal definitions of PR-STV. An article was published in Communications of the ACM, discussing the security issues associated with remote electronic voting. I have been compiling a letter to send by post to Mr. William Stapleton, requesting more detailed information, because I believe that e-mail is not taken as seriously as land-mail. I have been writing the research report, and have updated my website regularly. I have been learning  $\text{\LaTeX}$  for the research report and the letter.

## **Friday 31st of January**

Over Christmas I found the legal definition of PR-STV, which was suitably formal to develop flowcharts from. I read a paper published by the British government called “e-Voting Security Study”. It appears that the British government are seriously considering the introduction of voting via SMS text messages (among other things). Overall, the report was worrying in the attitude it took to security within electronic voting systems. I prepared a Gantt chart, detailing my remaining tasks. The research phase of this project has taken longer than expected. I learned how to use the Bibtex application, to prepare my bibliographies. I sent a second letter to Mr. Stapleton at the DoELG, requesting the Zerflow report under the Freedom of Information Act. I completed the first draft of the research report, and updated my website regularly.

## Thursday 20th of February

We agreed in early February that the specifications would be written in CafeOBJ. I have been developing Perl and Java code to produce tests, and have been developing Java implementations of the current specifications. I have kept my journal and website up-to-date, and have submitted the first draft of the final year report.

## Appendix D

# Specifications, Implementations and Tests

There is a website for this project. All code developed during the project is available there. The URL is:

<http://minds.cs.may.ie/~lovelace/E-Voting/>

### Specifications – CafeOBJ

The following CafeOBJ specifications were developed.

**Vote.mod**    <http://minds.cs.may.ie/~lovelace/E-Voting/src/Vote.mod>

**Votes.mod**   <http://minds.cs.may.ie/~lovelace/E-Voting/src/Votes.mod>

### Implementations

The following Java implementations of the specifications were developed.

**Vote.java**    <http://minds.cs.may.ie/~lovelace/E-Voting/src/Vote.java>

**Votes.java**   <http://minds.cs.may.ie/~lovelace/E-Voting/src/Votes.java>

## Tests

The following Java class and Perl scripts were used to build tests from the CafeOBJ specifications for both the specifications and implementations.

<b>VoteIO.java</b>	<a href="http://minds.cs.may.ie/~lovelace/E-Voting/src/VoteIO.java">http://minds.cs.may.ie/~lovelace/E-Voting/src/VoteIO.java</a>
<b>all_complete.pl</b>	<a href="http://minds.cs.may.ie/~lovelace/E-Voting/src/all_complete.pl">http://minds.cs.may.ie/~lovelace/E-Voting/src/all_complete.pl</a>
<b>all_incomplete.pl</b>	<a href="http://minds.cs.may.ie/~lovelace/E-Voting/src/all_incomplete.pl">http://minds.cs.may.ie/~lovelace/E-Voting/src/all_incomplete.pl</a>

## Appendix E

# Research Report