Submission of the Irish Computer Society to the Independent Commission on Electronic Voting and Counting at Elections on the secrecy and accuracy of the Nedap/Powervote electronic voting system and the testing thereof.

25 March, 2004.

Introduction.

The ICS's stance is that it is in favour of electronic voting in principle. The benefits of a properly implemented system include:

- improved accuracy compared to manually counted ballots;
- the elimination of unintentionally spoiled votes;
- faster counts, which may in turn make it possible to put matters to the people in referenda more often, thereby improving the quality of our democracy;
- the potential to improve accessibility and privacy for persons with visual impairment, reading difficulties, etc.

However, the proposed Nedap/Powervote system contains a fundamental design flaw which renders it unfit for use in elections and referenda, namely that it does not incorporate any means to independently verify the results it produces. As is explained below, computer systems are inherently error prone, and must be assumed to contain defects regardless of how thoroughly they have been tested.

We have deliberately not addressed the possibility of malicious attempts to tamper with the voting system for the purpose of electoral fraud. This is not because we discount the possibility, but because the provision of a means to audit election results for system error would also be sufficient to detect and deter attempted fraud.

Accuracy of the Nedap/Powervote system.

This ICS submission is based on a fundamental observation over more than thirty years of computing – that no amount of testing and/or review is sufficient to guarantee that any given computer system has no operational failure modes undetected by test, but discoverable in use. As the world-renowned computer scientist, the late E.W. Dijkstra (1972) put it, "testing can be used to show the presence of bugs, but never to show their absence!" This is because for all but the most trivial applications, the number of possible inputs to a computer program and possible paths through that program are so great as to make exhaustive testing of all the ways the program could be executed a practical impossibility.

This is not to say that software testing is pointless, but rather that a successful system test should be regarded merely as a pre-qualification for that system being used at all, within an overall context of cross-checks and assurances – not as proof that the system is entirely error free and that it will always work correctly in all circumstances.

According to the Department of the Environment (2002), the counting software proposed for use in Ireland contains approximately 200,000 lines of code. Based on industry standard figures[1], we can reasonably assume this software to contain defects which will result in anywhere between 30 and 120 serious system failures, or on the most optimistic view of its quality, a minimum of 10 such failures during its lifespan. We have no information to hand on the size of the code base for the embedded software in the Nedap voting machine, but it would be likewise reasonable to assume similar failure rates for it.

It is important to note that not all software system failures are immediately obvious to the operator – many can be extremely subtle and difficult or impossible to detect in use. They may also take a long time, possibly years, to manifest themselves. This is further complicated in the case of election software, where due to the secrecy of the ballot, the input to the software is by definition unknown by any party other than the voter.

Furthermore, hardware failures are inevitable in any physical machinery. The existence of computer hardware maintenance, repair, and data recovery companies demonstrates the everyday acceptance of the certainty of such failures. As with software failures, it would be naïve to assume that computer hardware failures will always be obvious.

The conclusion is inescapable that there is every possibility that undetected error, either in the voting machines used in polling stations or those in the count centre, may erroneously affect the outcome of Irish elections and referenda, unless there is some means of independently verifying their function.

It is our contention that for these reasons, any electronic voting system must include a paper-based voter verified audit trail. By this is meant that when voters cast their votes on an electronic voting machine a permanent paper record of their votes must be made, which can be securely checked by voters before the electronic record is made of the vote. The paper records must be retained and used in a number of randomly selected constituencies at each election to audit the accuracy of the electronically prepared result, as well as in any cases where a result is in dispute. Where there is a discrepancy between the paper and electronic records, the voter-verified paper version must take precedence. The audit trail must be voter verified, as the individual voters are the only people entitled to know how their votes were cast and therefore confirm the accuracy of the records made. Statistically valid checks on the electronically prepared result must be carried out at every election and referendum in which the voting system is used. It is not sufficient to check at the first few elections or referenda and stop if no significant discrepancies are found. As noted above, it may take years for some potential system failures to occur.

[1] Authorities such as Hatton (1998) estimate that good quality commercial software will contain 3 to 6 defects per thousand lines of code and that the lowest defect rate achievable using best current software engineering practice is about 1 defect per thousand lines of code. Of these defects, 5% to 10% can on average be expected to manifest themselves as serious system failures during the life-cycle of the software.

After-the-fact printing of the ballots recorded electronically by individual voting machines is not a substitute for such an audit trail, for while this could be used to independently verify the operation of the counting software, there is no way to prove that votes have been accurately recorded in the first place without a voter verified paper record.

A further important reason for having a paper trail is as a continuous backup device that is safe from electronic interference. The Nedap machine records votes on a removable electronic module. A backup module is provided, but according to Department of the Environment (2002), "all votes cast are transferred to a backup ballot module inside the voting machine when the poll closes". What happens if there is a catastrophic failure of the primary ballot module *before* the poll closes? On the face of it, it would appear that all voters up to the time of the failure who have used the voting machine concerned would be disenfranchised. Likewise, less obvious memory corruption would be faithfully copied to the backup module.

Secrecy of the Nedap/Powervote system.

In our view there are two significant difficulties for voter secrecy with the Nedap voting machine:

(1) Provision for voters with visual impairment, reading difficulty, etc.

One of the potential benefits of introducing an electronic voting system is the improvement of accessibility and secrecy, in particular for visually impaired voters. Currently, these voters must ask an electoral official to complete ballot papers on their behalf, thereby losing the secrecy of their votes (and incidentally risking their instructions being misunderstood and their votes not being cast as they wish). It is hard to understand why provision is not being made for this group of voters, especially as in the functional specification of the Nedap voting machine, under the heading "Facility for visually impaired persons" it is stated that "there is an RS-232 port on every VM [voting machine], which can be connected to an external device. The output to this port corresponds to the preference buttons pressed. The external device has to convert this output to the spoken names of the candidates and their political party or to the referendum choices." We are not aware of any plans by the Department of the Environment to provide audio devices of the type mentioned and we deplore the lost opportunity to improve access and secrecy for visually impaired voters.

(2) Provision for voters who wish to abstain secretly.

At present, a voter who wishes to abstain secretly, while giving the appearance of having voted normally, has merely to either cast a blank ballot or deliberately spoil his or her vote. It is not difficult to imagine circumstances where one might reasonably wish to do this, say if one was being pressurized to vote contrary to one's beliefs by a relative, friend or employer. Logically, if the right to abstain exists, the same right to do so in secret applies as to the right to vote in secret. However, as the Department of the Environment (2002) states: “There can be no spoiled votes. The voter must select a preference or preferences before the machine will accept a vote when the ‘cast vote’ button is pressed.” Although the machine can be deactivated by an electoral official should the voter choose not to press the ‘cast vote’ button, that means that the abstention is no longer secret.

Conclusions.

(1) Accuracy.

In the absence of an independent means of verifying every exercise of the Nedap/Powervote system, its accuracy in ongoing use, as distinct from occasional test, is undeterminable by design and therefore the accuracy of every result it produces will be unknown.

The only practical means of carrying out such verification is by a voter verified audit trail. Such an audit trail also has the advantage of unequivocally demonstrating to the voters, many of whom will have little or no knowledge of computers, that their votes have been accurately recorded. Furthermore, it protects the electoral officials and makers of the voting systems against disputes about the accuracy of election counts, which in the absence of an audit trail will be impossible to disprove, but which will cast unanswerable doubts on the results.

It is the unanimous view of the electronic voting committee of the Irish Computer Society that under no circumstances whatsoever should any electronic voting system be implemented which does not include a voter verified audit trail.

(2) Secrecy.

- It is impossible to understand why the opportunity to extend the right of voting secretly to the visually impaired has not been taken, particularly since the Nedap voting machine is specifically designed to facilitate this.

- The inability to abstain secretly using the Nedap machine is a worrying diminution of the right to cast one’s vote as one sees fit in secret.

About the Irish Computer Society.

The Irish Computer Society (ICS) was founded in 1967 as the national body for Information and Communication Technology (ICT) Professionals in Ireland. Since its foundation the Society has promoted the continuous development of professional ICT knowledge and skills in Ireland by organising seminars, lectures and related activities.

The Society is a nominating body for the Industrial and Commercial Panel of Seanad Éireann.

The ICS is an active member of the Council of European Professional Informatics Societies (CEPIS). CEPIS maintains both formal and informal links with the European Union and is recognized as a non-governmental organization with consultative status by the Council of Europe.

The ICS is the national member society of the International Federation for Information Processing.

Author.

This submission has been prepared on behalf of the electronic voting committee of the ICS by Fintan Swanton, MSc CEng MICS MBCS, Chartered Engineer, with contributions by Patrick O'Beirne, BSc MA FICS. Queries regarding its content should be e-mailed to info@ics.ie

Membership of the electronic voting committee of the ICS.

The members of the committee, who are all serving or former members of the ICS Council, are as follows:

Joseph Kearns, BE BSc MICS.
Jeremiah Russell, MICS.
Patrick O'Beirne, BSc MA FICS.
Michael O'Duffy, FICS MIEI BComm DPA CEng.
Mary Sharp, BSc(Comp) MA CEng MIEI FICS.
Fintan Swanton, MSc CEng MICS MBCS.

References.

Department of the Environment (2002) 'Direct Vote Recording/Electronic Vote Counting System Information Paper' http://www.environ.ie/DOEI/DOEIPol.nsf/0/588f0ce7a372f8c480256b7c0042de9d/$FILE/Elect%20Voting%20Info%20paper.pdf (Accessed 23 March, 2004)

Dijkstra, E.W. (1972) ' Notes on Structured Programming' in Dahl, O.J., Dijkstra, E.W. & Hoare, C.A.R. *Structured programming,* London, Academic Press.

Hatton, L. (1998) 'Programming technology, reliability, safety and measurement', *IEE Computing & Control Engineering Journal*, Vol. 9, No. 1.