Appendix 2K

Experience with Voting Machines in the Netherlands and Germany

THE POLICY INSTITUTE, TRINITY COLLEGE DUBLIN

Dr. Kees Niemoller, *P&D Analytics, Alphen, The Netherlands*

Table of Contents

1 Introduction

It is the intention of the Irish government to introduce Electronic Voting at the European Elections in June 2004. Part of the introductory process has been the establishment of an advisory committee, the Commission on Electronic Voting, whose main task is "to prepare a number of reports for presentation to the Ceann Comhairle on the secrecy and accuracy of the chosen electronic voting and counting system i.e. the Powervote/NEDAP system".[1]

The Policy Institute, Trinity College, Dublin has, among others, been asked to study and report on several aspects of the Powervote/NEDAP system, including international experiences in using the system. As the NEDAP system for electronic voting is currently in use in more than 90 per cent of all polling stations in the Netherlands (and has been in use in some municipalities for approximately 30 years), consideration of the Dutch experiences were thought to be useful for the work of the Commission. In the short time available it did not prove possible to include information on other European countries as well, with the exception of experiences with electronic voting in Germany. In 2002, around 5, 000 NEDAP voting machines were in place in Germany and this report summarises the current practice and evaluations of these machines.

In the following sections, a number of topics concerning the use of electronic voting are presented. The report begins with a discussion of the legal context in the Netherlands of the use of electronic voting machines and summarises the main points of debate. In the second part of the report, a more detailed analysis is provided of the aspects relevant for the secrecy and accuracy of hard- and software of the NEDAP system. A third section considers recent experiences with the NEDAP voting machine in Germany. Finally, the conclusion summarises the report's main findings.

The findings are based on a desk study of the main scientific and non-scientific publications on the matter as well as, interviews with people from the Ministry of Interior, the Elections Advisory Board, NEDAP, the testing organisation TNO and Universities. A list of relevant publications reviewed and persons interviewed are detailed in Appendix One.

2 Voting machines in the Netherlands[2]

2.1 Basic principles

As in all other western democratic states, the election process in the Netherlands can be characterised by three important catchwords: correct, verifiable and secret. Correct means that only enfranchised people have voted, that each of them has cast only one vote and that only valid votes have been counted. The criterion of a secret ballot guarantees that it is impossible to relate a person to his or her vote. Furthermore, a voter should not be able to show proof of what he or she has voted. Finally, the results of an election should be verifiable for all people concerned.

[1] Terms of reference Commission on Electronic Voting (version of March 9, 2004).

[2] This section is mainly based on the following sources:
- Electoral law of the Netherlands
- Regulations of the Ministry of Home Affairs
- Interviews with the secretary of the Elections Advisory Board (Kiesraad) of the Ministry of Home Affairs
- Wolter Pieters (Security of Systems Group; Katholieke Universiteit van Nijmegen): Stemmachines in Nederland. September 2003.

The manner in which the State seeks to guarantee these basic principles is outlined in the Election Law. The Election Advisory Board, consisting of experts who have been appointed by the Minister of Interior, advises the Minister on matters concerning the elections and act as the main election office responsible for the organisation of the elections.

Interestingly enough, with regard to the *method of voting*, the majority of the articles in the Election Law still mention paper ballots and red pencils to be used by the voters on Election Day. The Law explicitly allows the use of methods other than pencil and paper, but it does not stipulate any details.

Details concerning the use of electronic voting are legally embedded in a so-called General Act of Government *(Algemene Maatregel van Bestuur)*, which is issued by the Cabinet and does not need to pass Parliament. Electronic voting was introduced in the Netherlands for the first time in an election in 1982, but it took a long time before the conditions for using and details on testing were legally embedded. A first General Act on Electronic Voting was issued in 1989 regulating the approval of voting machines. This Act was replaced by a more detailed Act issued in July 1997 by the Secretary of State for the Interior.[3] The most recent Act provides details on the testing of voting machines and refers to an independent test-institute. In the same year, TNO (TNO Electronic Products & Services B.V.) was officially appointed by the Ministry to conduct the testing of the hard- and soft-ware used in the voting machines.[4] Since then, electronic voting has twice been the object of government interest. Immediately following the local and parliamentary elections of 1998, the Secretary of State for the Interior asked the Elections Advisory Board to advise him on several matters concerning electronic voting. These matters were:

- The announcements of the first, temporary, election results;
- The possibility of a so called paper-trail for the individual voter;
- The need for more detailed regulations on the use of the software used to calculate the results; and
- The need to narrow the risks arising from the total dependency on the companies who deliver the hardware and software.

The Election Advisory Board hired an external consultant to assist them in providing advice on these issues and in 1999 the Parliament passed most of the recommendations made in the report issued by the consultant. Electronic voting was on the agenda of the Ministry of Interior for a second time in 2002. This arose from a number of problems experienced in the two elections that occurred during 2002 namely, with the software calculating the final distribution of seats. The Elections Advisory Board was asked for advice on the testing and approval of the software and in March 2003, the Board provided several recommendations in relation to the issue. The next section discusses in detail the use of voting machines in the Netherlands and presents the results of the aforementioned two studies.

2.2 Authorisation of voting machines

The 1997 General Act of Government on the use of voting machines regulates the conditions for the authorisation and valid use of the machines. In short, the authorisation process includes the

[3] Algemene Maatregel van Bestuur, *Regeling voorwaarden en goedkeuring stemmachines 1997*, Ministerie van Binnenlandse Zaken, 11 Juli 1997.

[4] TNO is a large research and technical orgnisation. Its mission is to make scientific knowledge applicable to strengthen the innovation capacities of business and government.

following:

(i) A potential manufacturer of a voting machine first of all develops a prototype that has to be tested by TNO, the only testing institute certified to do so. Once the prototype meets all the requirements, production may be started;

(ii) All voting machines produced are now subject to a one-out-of-every-ten test to check their compatibility with the prototype;

(iii) Test-reports are sent to the Ministry of Interior and the final permission to use a machine is given by the Minister; and

(iv) At least once every four years, a sample of voting machines is tested again to assure their proper functioning. Between 1998 several companies competed for governmental authorisation and were formally approved: NEDAP (ES3B and ES3A1), Alcatell Bell (ES-Vote, under conditions), Control Systems-Van Rietschoten-Houwens Noord West B.V. in 1998; Alcatell Bell c.s. (ES-Vote 2.3) and NEDAP (ES3B V.2.10) in 1999 and NEDAP (ES3A1 and ES3B V.2.11; EDS-1 V3.0) in 2002.

It is the choice of the Municipal government in the first instance to decide whether to discard the traditional method of voting by paper and red pencil and to introduce electronic voting and, secondly, which (authorised) type of machines to buy. After purchase, the municipality and the polling station subsequently control the proper functioning of the voting machines.

The introduction and use of electronic voting machines in the Netherlands was rather uneventful, since all relevant actors agreed on the advantages of such a system (NEDAP or other brands). The main advantages were seen to be as follows:

- Reduction in the number of polling stations;
- Reduction in the number people necessary to attend the polling stations;
- Improvements in electoral administration;
- Production of more accurate and earlier results; and
- Avoiding the casting of invalid votes.

Local governments underlined these advantages and, in browsing through the records of the local councils, it is obvious that city councillors had only one major problem with the decision to switch over to electronic voting, namely the costs. It becomes clear that once a community changed to electronic voting, the benefits outlined above were observed as expected.

All this is demonstrated in the study initiated by the Elections Advisory Board in 1999.[5] In this study, 47 communities were approached with a number of questions. Twenty of these communities used the NEDAP voting machine, 15 used machines from other brands and 12 communities followed the traditional paper ballot procedure. Of the 20 communities that used the NEDAP system, four had a machine from before 1990, six used machines since 1994 and the others used machines since 1998. The main reasons driving the switch to voting machines that were mentioned were as follows:

1. Increase the efficiency of the polling stations (no reason for a recount and the inherent possibility of errors);
2. Reduction of costs for the construction and arrangement of the polling station; and
3. Earlier presentation of final results.

[5] Stand van zaken automatisering rond verkiezingsproces. Het Expertise Centrum. 1999.

Furthermore, 80 per cent of the Municipalities indicated that the introduction of the voting machines resulted in a 25 per cent (on average) reduction in the number of polling stations. All 20 communities were satisfied with the performance of the voting machines and the technical support by NEDAP. The study also found that the number of failures or malfunctions was very small. In general, these failures occurred immediately after the machine was bought or were caused by lack of knowledge on the part of the attending personnel. Machines bought in 1994 or later showed hardly any problems at all. A final observation is that 60 per cent of the communities were of the opinion that the use of a voting machine took less time than the traditional method of voting with paper ballots.

2.3 Debates

Based on the interviews conducted and the two advisory reports of the Elections Advisory Board, it is possible to distinguish a number of issues that are the subject of debate, namely:

(i) The public availability of the so called source codes;
(ii) The lack of a voter verified audit (paper) trail; and
(iii) The authorisation of the software for the distribution of seats.[6]

2.3.1 Source code

The main issue under debate in relation to this is whether the source codes should be published. In the Netherlands, the two types of software, the embedded machine software and the counting software, are treated differently. The embedded software is tested by NEDAP itself and TNO, the only accredited test institute in the Netherlands. The test reports are submitted to the Minister of Interior who then decides whether or not to authorise the machines. The testing organisation has, of course, full access to the software, which contains numerous lines of comment to facilitate the analysis of the code.

Knowledge of the source code is restricted to a limited number of persons, all specialists and some of them from an accredited institution and of immaculate reputation. So far, according to the interviewed persons and reports, the integrity and quality of these institutions have not been doubted, but there are some people who would like to see the source codes made known to a wider range of people. The idea is that publishing the source code would make detection of possible malicious changes made by compromised programmers more likely. However, NEDAP is not willing to publish the embedded software for fear of losing their market to competitors who would copycat their voting machine.

It should be pointed out that even when the source codes are made public, problems might not necessarily be detected easily or even detected at all. Prof. Dr. Bart Jacobs stresses the importance of ensuring that software should be *correct* and *secure*.[7] A computer program is correct (or safe) if, under normal conditions, it performs as it is supposed to do. Software is secure if the program always functions in a proper way, even under conditions of malpractice: security is safety under attack. According to Jacobs, large computer programs cannot be analysed and tested adequately. The number of possibilities is so large that only special computer programs with model checkers or

[6] Website of Rebecca Mercuri: www.notablesoftware.com
Margaret McGaley and Dr. J. Paul Gibson. Electronic Voting: A Safety Critical System. 2003
Website of Peter Knoppers: ce.et.tudelft.nl/~knop/stemmachines/ (in Dutch)

[7] Bart Jacobs. De computer de wet gesteld. Oratie, Nijmegen 2003.

theorem proving can help with the systematical control of all possibilities that could occur within the software. However, in his opinion, these formal, mathematical methods can be used for very small programs only. To test the correctness of larger programs, one is dependent on less encompassing methods like tests, inspection of the code and systematical design.

NEDAP is far less restrictive with regard to the source code for the counting and tabulation software. On the contrary: not only do test institutes have access to the code, NEDAP also deposited the source code in the office of the Election Advisory Board and made similar provisions with the Association of Users (Dutch communities using NEDAP's voting machines).

2.3.2 Voter verified audit trail

A second issue relates to the desirability of a so-called Voter Verified Audit or paper trail. At present, the NEDAP machines do not provide a paper trail. Voters can control their initial vote on a display and then decide whether to cast their vote or change it. After closing time, the voting machine produces a complete paper audit of all the votes and the officials of the polling station check the total with the number of ballot papers. However, according to Mercuri, the voting system should print a paper ballot containing the selections made on the computer. "This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises".[8] This would ensure that it was possible to compare the results of (a sample of) voting machines with a paper ballot. In the event of a discrepancy occurring, the paper ballot would be considered the official vote and the tabulation made by the voting machine as 'unreliable'.

To-date, NEDAP has resisted the demand for a paper trail by referring to the technical problems that the use of printers in the machines would cause. NEDAP argues that printers are notoriously vulnerable and that when a cast vote would not be (properly) printed, serious problems would arise during Election Day. Even more problematic, according to the spokesmen of NEDAP, would be the fact that the paper ballot would be considered the official vote, even when there are doubts about the reliability of the verification by voters of the paper ballot. Some voters are not interested and will not check the printed vote at all, while others, noting a discrepancy, might think they made a mistake or would not want to start a discussion on the issue with the personnel of the polling station.

The arguments put forward by NEDAP in relation to this are affirmed by a number of American IT experts. Recently, the four principal authors of the Help America Vote Act (HAVA; signed on October 29 2002 by President Bush) addressed the Congress of the United States in a letter to express their concern about "recent legislative efforts that promise enhanced electronic voting system security" as follows:

> *"Various proposals have been introduced in the House and Senate, but a common feature of these bills is they would amend HAVA to require that all voting systems, including electronic and computer-based systems, produce or accommodate a 'voter verified paper record'. Not only are such proposals premature, but they would undermine essential HAVA provisions, such as the disability and language minority access requirements, and could result in more, rather than less, voter disenfranchisement and error. […] While there are risks associated with any technology, the solution is not to rush to judgment by returning to flawed systems. Rather, the answer is to allow the Commission, together with the active*

[8] Rebecca Mercuri. A Better Ballot Box? IEEE Spectrum Online, 2002.

> *input of election officials, computer experts, and civil rights groups representing voter interest, to develop standards for ensuring the security of all voting systems, as required under HAVA."* [9]

NEDAP's thinking, as became clear in the interviews conducted by the author with its representatives, runs along very similar lines as those outlined above in the quote from the HAVA representatives. Instead of introducing a paper trail in the machines, they would opt for camera screening (without breaching the secrecy of the ballot) of the voting acts in randomly selected polling stations. The outcome of the screening could then be compared with the calculations of the voting machines.[10]

One of the strongest opponents of the use of voting machines (of any brand), Mr. Peter Knoppers from the Technical University of Delft (who devotes a very critical website to the subject[11]), mentions a recent development: a voting system with a very special printer as proposed and described by David Chaum.[12] However, Knoppers admits that Chaum's system, and especially the printer, would be even more vulnerable. It is also expensive.

2.3.3 Software for the distribution of seats

The third issue relates to the software for calculating the final distribution of seats. The Elections Advisory Board advised the Ministry of Home Affairs in 2003 about the desirability of tests for software for the calculation of the distribution of seats.[13] The report begins by explicitly stating that there was no reason to suppose that the software used for the calculation of seats did not conform with the regulations. The Elections Advisory Board itself observed that in the past the software was tested many times and that results of the tests have been used to make adaptations to the software. Nevertheless, the Board was of the opinion that they should be as vigilant as possible, not only to boost the faith of the public, but also because at two polling stations (in 2002 and 2003) small differences were detected. The Advisory Board therefore advised the Minister of Interior: "To have a test developed for approving the software for the counting and the distribution of the seats to parties and candidates. Criteria for approval should be restricted to a minimum necessary to guarantee the proper functioning of the software". Furthermore, the Board stressed that all software used for the counting and the distribution of the seats to parties and candidates should be open for testing including the software used by the communities to count and calculate the local results as well.[14] At this point in time, such a test is not part of the regulations. Another recommendation of the Election Advisory Board is that 'Proper functioning of the software should be tested by a 'black box method' using test sets with a known outcome (e.g. election data from the past)'. That means that the Board, given the development of the software market, does not want a line-by-line source code analysis. The testing of the software should be done under the direct responsibility of the Minister of Home Affairs and not, as is the case for voting machines, by an outside institution like TNO.

Overall, this section has described the Dutch context with regard to the use of electronic voting

[9] Letter to the Congress of the United States, March 3, 2004.
[10] Oral communication by NEDAP spokesmen.
[11] URL: ce.et.tudelft.nl/~knop/stemmachines/
[12] David Chaum. *Secret-Ballot Receipts and Transparent Integrity. Better and less-costly electronic voting at polling places*. Article can be downloaded at ce.et.tudelft.nl/~knop/stemmachines/
[13] This advice was based on an external consultancy report carried out by Het Expertise centrum. See *Goedkeuring Software Zetelverdeling*. Het Expertise Centrum, 2000.
[14] In practise, only one software package is used.

machines. The next section provides a more detailed report on the different aspects of the NEDAP machines.

3 NEDAP Electronic Voting Machines

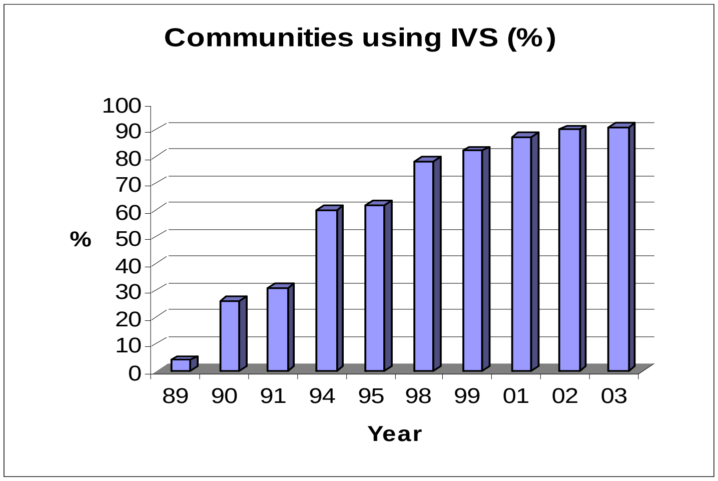
3.1 The use of Nedap electronic voting machines on Election Day(s)

During the last parliamentary elections in The Netherlands in 2003, 85 per cent of the voters voted by means of an electronic voting system. Of these, 95 per cent were confronted with the Integrated Vote System (IVS) of NEDAP, a Dutch company that is a major player on the European market for electronic voting systems. The IVS is an integrated system, composed of a machine and specially developed software.

The method of voting, electronically by machines, received little attention in the Dutch newspapers. This was probably largely due to the fact that only five of the total of 7,500 vote machines had manifest problems and these were resolved before the polling stations opened their doors. Furthermore, minor problems that occurred during Election Day were remedied by NEDAP-staff stationed at 70 locations throughout the country. Company policy is that if a voting machine is out of order, it has to be replaced within 30 minutes. It turned out that these 70 support units were sufficient, while for some of the Dutch islands, a spare machine was already in place.

Over the last 30 years, more and more local governments have decided to use NEDAP machines and IVS and especially during election years, the percentage of communities using IVS has increased. Interestingly enough, citizens of the capital of the Netherlands, Amsterdam, still vote with a red pencil. At first the reason was the decentralised structure of the city as, especially at local elections, people had to vote twice: once for the city council and once for the district council. However, the newest generation of voting machines can handle more than one election. The reason now to prefer paper ballots and the red pencil (or red lipstick which is explicitly allowed by the Election Law!) is that the city of Amsterdam prefers to wait for the next phase in technical developments, i.e. virtual polling stations (PC-Internet etc). Another city in the Netherlands, Arnhem, continues to use the red pencil for financial and 'nostalgic' reasons.

Figure 1. Percentage of municipalities using IVS



The municipalities store the voting machines once acquired. The machines require no special maintenance and on Election Day they are transported to the polling stations. On behalf of the Election Advisory Board, who acts as the main Electoral Office during the elections, NEDAP merges and checks the lists of candidates of each party. The Municipality takes care of the programming of the Ballot Module (see below). The Ballot Module is used on Election Day by the chairperson of a polling station to activate the voting machine.

On Election Day a voter presents his/her ‘summon' for the election. This summon is then compared with the voting register, after which the voter receives a serial number that must be given to the person that operates the voting machine. Next, the voting machine is unlocked and the voter casts his/her vote. On the service panel of each voting machine there is a print of the ballot paper. When a voter pushes the button next to a candidate’s name, that name and the name of the political party becomes visible in a display and the voter then can either cast his or her vote or decide to change it.

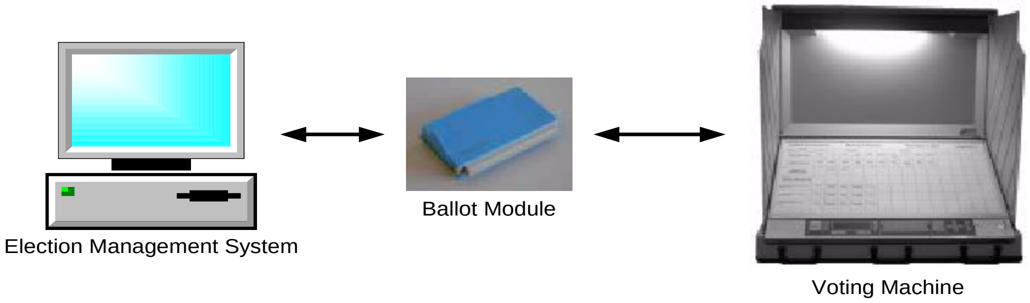
At the closing time of the polling station, the chairperson instructs the voting machine to print a complete audit with the number of votes for each candidate, the total number of votes for each party, the total number of voters that made use of the voting machine, the total number of so-called blank votes and the total number of valid- and not-valid votes. This paper audit is transferred to the main election office of the Municipality. Separately, the Ballot Module is brought to the main election office and by means of a special connecting device the data are fed into a PC and converted into the election result for that community.

To safeguard the continuity of the use of the electronic voting machines, the Municipalities are organised in an association of users of NEDAP voting machines where NEDAP deposited a protocol of the software (not the software embedded in the voting machine itself). In case NEDAP would discontinue its services, the Association is allowed to search for another company to facilitate the use of the software. The annual reports, however, indicate that so far there is no friction between NEDAP and the Municipalities using ISV.

3.2 The NEDAP voting machines

The election system consists of an Election Management System (EMS) and the NEDAP Voting Machine (VM). Communication between the VM and the EMS happens through transportable ballot modules (BM). The EMS is used to define elections for all election districts of a county, including offices, candidates, affiliated political parties and propositions used in referendums. The EMS is responsible for programming the BM and providing the correct information for printing the ballot paper facings. Programming is done in the programmer-reader unit connected to the EMS.

Figure 2. NEDAP voting machines



Source: NEDAP

The BM is responsible for securely transporting the election definition to the VM and the votes cast into the EMS. For this reason, a BM consists of two EPROMs in which the votes are stored redundantly with security checks. Voters make their choices using the VM: first, they push a button to select the desired candidate; they then verify the choice on the display; and finally, push the vote-cast-button. A second BM in the voting machine is not transportable and is used, after the polling is closed, to copy the entire data of the transportable BM before it is brought to the EMS again.

An important issue is, of course, how secure and secret the machines are. As mentioned in the previous section, the hardware and software are tested by TNO but these testing reports are not available to the public. For the purpose of this report, interviews were conducted with two representatives from NEDAP. These interviews explored with the NEDAP representatives, the criteria published by Peter Neumann (1993) concerning "confidentiality, integrity, availability, reliability, and assurance" for computer systems involved in electronic voting.[15] Neumann suggests that these are generic electronic voting criteria, although he also concludes "an assessment of the realizability of those criteria leads to the conclusion that, operationally, many of the criteria are inherently unsatisfiable with any meaningful assurance." In the following sections, the report considers the NEDAP voting machine in light of these criteria (stated in italics), bearing in mind Neumann's warning, and the fact that the machine is not a PC, which makes a number of criteria less meaningful or even not applicable.[16]

a) System integrity.

The computer systems (in hardware and system software) must be tamperproof. Ideally, system changes must be prohibited throughout the active stages of the election process.

NEDAP voting machines are stand-alone systems with embedded software that is not changeable without notice (covered and sealed). The software resides in EPROM, there is no hard disc or floppy drive. The machines are copies of those that were certified by the accredited bodies.

b) Data integrity and reliability.

All data involved in entering and tabulating votes must be tamperproof. Votes must be recorded correctly.

All relevant election data is protected by an error-detection code. Votes are stored twice in two physically independent memory devices, so every vote is stored four times. Whenever there is a discrepancy, the voting machine is locked and cannot be used anymore except for reading the Ballot Module and the contents recorded on the BM as of that moment in time.

c) Voter anonymity and data confidentiality.

The voting counts must be protected from external reading during the voting process.

The association between recorded votes and the identity of the voter must be completely unknown within the voting systems.

During the voting process, counting is disabled. Once counting has started, the voting process cannot be re-started. Votes are stored randomly into the memory devices so it is considered impossible to associate a recorded vote and the identity of a voter.

d) Operator authentication.

All people authorised to administer an election must gain access with nontrivial authentication

[15] Peter G. Neumann. Security Criteria for Electronic Voting. Paper presented at the 16th National Computer Security Conference Baltimore, Maryland, September 20-23 1993.

[16] In the left column, Neumann's criteria are summarised. The right column is the result of analysis of test-documents, interviews with NEDAP-staff and written comment given by NEDAP on our request.

mechanisms. Fixed passwords are generally not adequate. There must be no trapdoors --- for example, for maintenance and set-up --- that could be used for operational subversions.
The system is only operable by using two different physical keys owned by two authorised people. The local authorities that are responsible for the operation of the voting machine appoint these persons.

e) System accountability.
All internal operations must be monitored, without violating voter confidentiality. Monitoring must include votes recorded and votes tabulated, and all system programming and administrative operations such as pre- and post-election testing. All attempted and successful changes to configuration status (especially those in violation of the static system integrity requirement) must be noted.
System operation is monitored on the display control unit, without displaying choices made by the voter. All changes in modes (e.g. from standby to voting mode, from standby to counting mode, etc) are recorded. This is recorded in a special memory device and can be printed in a special mode. All election data and stored votes are continuously tested on integrity (i.e. that they have not been tampered with).

f) System disclosability.
The system software, hardware, micro code, and any custom circuitry must be open for random inspection at any time (including documentation), despite cries for secrecy from the system vendors.
The whole system including the source code is open for inspection at any time by an accredited body, namely TNO and PTB. Any random chosen system can be disposed to such an organisation for verification. In The Netherlands, TNO performed these tests. The German test-institute, PTB in Berlin, also performs software tests in the form of a line-by-line code inspection.

g) System availability.
The system must be protected against both accidental and malicious denials of service, and must be available for use whenever it is expected to be operational.
The system is maintenance free and operable at any time. There are no ‘deadly’ key-combinations (i.e. the equivalent of control-alt-del).

h) System reliability.
System development (design, implementation, maintenance, etc.) should attempt to minimise the likelihood of accidental system bugs and malicious code.
Structured design: requirements, functional specification, implementation specification and test specification are basic parts of the system development. The system is designed with sub-circuits whose functions are testable for diagnostic (self) tests.

i) Interface usability.
Systems must be amenable to easy use by local election officials, and must not necessitate the on-line control of external personnel (such as vendor-supplied operators). The interface to the system should be inherently fail-safe, fool-proof, and overly cautious in defending against accidental and intentional misuse.
The system is stand-alone and easy to operate by just a few simple operations.
The user manual of the system is very detailed.[17] There are no vendor-supplied operators and NEDAP’s role is mainly restricted to the replacement of a blocked machine.

[17] Handleiding Integraal Stemsysteem voor Windows. NEDAP/Groenendaal.

j) Documentation and assurance.
The design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented. Documentation must also describe what assurance measures have been applied to each of those system aspects.
Documentation: requirements, functional specifications, software design, hardware design including Worst-Case Analysis, Failure Mode and Effect Analysis, hardware and software test plans, test descriptions and test results. Test reports on software, hardware, EMC, safety and environmental tests from independent authorities are available.

k) Personnel integrity.
People involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity. For example, convicted felons and gambling entrepreneurs are suspect.
Every person involved with the voting machine is screened by NEDAP or by the municipality.

3.2.1 System trustworthiness

a) Security vulnerabilities are *ubiquitous in existing computer systems, and also inevitable in all voting systems --- including both dedicated and operating-system-based applications. Vulnerabilities are particularly likely in voting systems developed inexpensively enough to find widespread use.*
Proprietary hardware and software ensures control of every aspect in the design. The embedded software is developed exclusively for the voting machine and is not used in any other system (NEDAP or otherwise). The software resides in EPROM: there is no external access to the system.

b) System operation *is a serious source of vulnerabilities, with respect to integrity, availability, and in some cases confidentiality --- even if a system as delivered appears to be in an untampered form. A system can have its integrity compromised through malicious system operations --- for example, by the insertion of Trojan horses or trapdoors. The presence of a* **superuser** *mechanism presents many opportunities for subversion. Furthermore, Trojan horses and trapdoors are not necessarily static; they may appear only for brief instants of time, and remain totally invisible at other times.*
System operation of the voting machine is very simple with easy to perform checks before, during and after the election on its integrity. Before the election, verification on programming of the ballot images and number of votes recorded (should be zero) has to be performed. During the election, the number of votes can be verified with the number of tickets used for ‘parallel’ counting. The voting machine is not a PC-based system.

c) System integrity *can be enhanced by the use of locally non-modifiable read-only and once-writable memories, particularly for system programs and preset configuration data, respectively.*
System program resides in EPROM and cannot be reprogrammed in the machine. The ballot module is pre-programmed with election configuration and election data. It includes checksums for testing its integrity.

d) Data confidentiality, integrity, and reliability *can be subverted as a result of compromises of system integrity. Non-alterable (e.g., once-writable) media may provide some assistance for integrity, but not if the system itself is subvertible.*

Election data and votes are stored in the ballot module. Votes can only be added to the ballot module. Re-writing is only possible after erasing the device (i.e. to enable it to be used in a new election/referendum). The special construction of the hardware avoids the possibility that an unwanted erase command of the transportable ballot module can be generated. Erasing of this module is only possible outside of the voting machine (in the programmer-reader unit). The backup module can be erased inside the machine.

***e) Voter anonymity** can be achieved by masking the identity of each voter so that no reverse association can be made.*
No detail of the identity of the voter is registered in the voting machine. Only the vote is recorded, without any link to the voter's identity. A random generator ensures that votes are stored in the memories at random.

***f) Operator authentication** must no longer rely on sharable fixed passwords, which are too easily compromised in a wide variety of ways. Some other type of authentication scheme is necessary, such as a biometric or token approach, although even those schemes themselves have recognised vulnerabilities.*
During the election in the polling station at least two (official) persons are present. Two operators each with a different key are needed to operate the machine. This avoids fraudulent actions taken by only one person.

***g) System disclosability** is important because proprietary voting systems are inherently suspect. However, system inspection is by itself inadequate to prevent stealthy Trojan horses, run-time system alterations, self-modifying code, data interpreted as code, other code or data subversions, and intentional or accidental discrepancies between documentation and code.*
Besides in-depth line-by-line code inspection by accredited bodies (TNO in The Netherlands and PTB in Germany), election end-to-end tests can always be set-up by independent parties. After each alteration to the system, extensive end-to-end tests are run by NEDAP or outside institutions. For example, NEDAP/Powervote's Integrated Election System Irish-rules STV software (IES) was tested by comparing the output of several hundred IES election result sheets with those generated by the Electoral Reform Services program, eSTV, when given the same vote data files. The testing was successful.[18]

3.2.2 System Robustness

***a) System availability** can be enhanced by various techniques for increasing hardware-fault tolerance and system security. However, none of these techniques is guaranteed.*
The robustness of the voting machine is tested by a number of environmental tests performed by TNO (vibration, shock, topple, free-fall, temperature and humidity). TNO also test extensively the electro-magnetic compatibility (for example electrostatic discharge, thunderstorm, cattle prods etc.). At the request of NEDAP, TNO raised the criterion from 8kV to 16kV. Many years of experience shows a high availability of the systems (i.e. that the systems are very sturdy and have passed many rigorous tests to ensure that the machine is not likely to break down).

***b) System reliability** is aided by properly used modern software-engineering techniques, which can result in fewer bugs and greater assurance. Analysis techniques such as thorough testing and high-assurance methods can contribute. Nevertheless, some bugs are likely to remain.*
The software is properly designed and thoroughly inspected (line-by-line) by an accredited body (ISO/IEC 17025).

***c) Use of redundancy** can in principle improve both reliability and security. It is tempting to believe that checks and balances can help satisfy some of the above criteria. However, we rapidly*

[18] Joe Wadsworth and Brian Wichmann. Report on Irish STV Software Testing. 2003

discover that the redundancy management itself introduces further complexity and further potential vulnerabilities. For example, triple-modular redundancy could be contemplated, providing three different systems and accepting the results if two out of three agree.
The ballot module has two physically independent circuits (drivers and memory devices). The votes are stored twice in each memory device. Every choice made is directly expanded with an error detection code. All definite four-vote parts have error detection code added. Whenever an error is detected, the voting machine is locked and cannot be used anymore (although the ballot module can be read elsewhere so that votes stored in memory are not lost).

d) Interface usability *is a secondary consideration in many fielded systems. Complicated operator interfaces are inherently risky, because they induce accidents and can mask hidden functionality.*
The user interface is very simple and supported by display messages.

e) Correctness *is a mythical beast. In reliable systems, a probability of failure of 10^{-4} or 10^{-9} per hour may be required. However, such measures are too weak for voting systems. For example, a one-bit error in memory might result in the loss or gain of 2**k votes (for example, 1024 or 65,536). Ideally, numerical errors attributable to hardware and software must not be tolerated, although a few errors in reading cards may be acceptable within narrow ranges.*
Efforts must be made to detect errors attributable to the hardware through fault-tolerance techniques or software consistency checks. Any detected but un-correctable errors must be monitored, forcing a controlled rerun.
However, a policy that permits any detected inconsistencies to invalidate election results would be very dangerous, because it might encourage denial-of-service attacks by the expected losers.
In the Netherlands, a failure rate of less than 10^{-6} is required. Calculation made by TNO shows a failure rate of less than 10^{-13}. All relevant circuits are testable. Diagnostic tests (i.e. data and address line checks, integrity of the votes, RAM and ROM checks) are implemented and continuously performed. Misbehaviour is recorded (and should this occur), the machine will be blocked and (within 30 minutes) replaced by another voting machine.

3.2.3 System Assurance

a) High-assurance systems *demand discipline and professional maturity not previously found in commercial voting systems (and, indeed, not found in most commercial operating systems and application software). High-assurance systems typically cost considerably more than conventional systems in the short term, but have the potential for payoff in the long term.*
NEDAP has built voting machines since 1970. For the first 10 years it was a completely mechanical machine and NEDAP learned a considerable amount about the mechanical parts of the machine. Together with the next 25 years of designing and producing electronic voting machines, NEDAP has gathered considerable knowledge on how best to assure the provision of a secure and reliable voting machine. It is estimated that throughout these years, 60 million votes have been recorded without any problem.

b) User friendliness.
In addition to these ‘formal’ criteria, according to the representatives from NEDAP, the users of the voting machines have fewer complaints than they had when using the traditional paper ballot procedure e.g. the print with the names of the parties and the candidates is easier to read because it is bigger than a ballot paper; for visually handicapped, a magnifying glass is attached to the machine; mistakes can be corrected by simply pushing the button of another candidate; and, pressing a button is easier than the exact coloring of a circle by means of a red pencil attached with a string to the polling booth.

4 Electronic voting in Germany

In Germany, the Election Law was adapted in 1975 to allow the use of mechanical- and electronic voting machines. In 1998, NEDAP voting machines were tested for the first time in Cologne. The tests were evaluated by the City Council as very successful and one year later, the elections for the European Parliament in Cologne were carried out exclusively with (600) NEDAP voting systems. In the following years, other cities followed: in the elections for the Bundestag of 22 September 2002, 29 Municipalities used the NEDAP electronic voting machines.

A desk study of the main scientific and non-scientific publications on the matter, as well as interviews with people from the Election Bureau in Cologne leads to the conclusion that the present state of affairs in Germany resembles the situation as it was in The Netherlands some years ago. For example, the election law was adapted a couple of times to allow the use of voting machines'; the number of communities that use a voting machine is steadily growing; a number of large cities (Köln, Düsseldorf) have used voting machines for quite a number of elections; it is the decision of local governments to introduce and finance voting machines; only machines authorised by the Minister of Interior are permitted and the market is dominated by one system, the voting machine of NEDAP. Furthermore, there is little debate on the use of voting machines, even about the two topics that caused some stir elsewhere namely, the secret source code and the lack of a voter verified audit trail.

It appears that when making the decision to switch to using electronic voting, Community councils are primarily concerned with the financial aspects e.g. cost per machine, reduction of the number of polling stations and polling station personnel.

There exists a widespread trust in the accuracy and safety of the NEDAP voting machines. The German testing institute, the Physikalisch-Technischen Bundesanstalt (PTB) has an excellent (international) reputation and its authority is widely accepted. Their test of the NEDAP system is even more extended and thorough than that of TNO in the Netherlands, especially with regard to the line-by-line code inspection and design/structure analysis of the software.

Although the PTB test reports were not available to us, the testing concept is known. In a lecture, Prof. Dr. Dieter Richter (2001) from PTB discussed the principles- and operating procedures of the testing of voting machines.[19] According to Richter there are many components in the test concept of PTB, such as: the electromagnetic compatibility, insusceptibility of the apparatus, stability of the system under mechanical impact, the ergonomics of the service panel, the security in a situation of power failure, the insusceptibility for mistreatment, the protection against repeated voting by the same person, and protection against any manipulation of hard- and software. Special attention is paid to the testing of the software: correctness, reliability and protection against manipulation are of the utmost importance. Based on legal demands and the technical norms for high-security software testing, a catalog of more than 50 software characteristics is deduced.

All in all, PTB is confident that the voting machines are adequately tested and experiences with the system in the field (e.g. elections) give PTB no cause for adaptation of the test concept.

[19] Prof. Dr. Dieter Richter (PTB). Lehren aus der Wahlgeräteprüfung für Online-Wahlen. Erweiterte Fassung des Kurzvortrages anlässlich der Workshops „Online-Wahlen“ beim Bundesministerium der Innern, Berlin, 11 December 2001, erarbeitet unter Mitwirkung von Herrn Dr. Volker Hartmann und unter Verwendung von Materialen von Herrn Dr. Norbert Greif, beide PTB.

4.1 Evaluation

As well as the tests of the system described in the section above, there exists a number of extensive evaluations of the experiences with the voting machines of NEDAP in Germany. The University of Koblenz-Landau undertook of a meta-analysis of 13 different surveys in 13 Municipalities as well as their own research on the use of electronic voting machines in Rheinland-Pfalz.[20] The principal findings from both the meta-analysis and separate research study are summarised below.

The meta-analysis report analyses 13 separate evaluations of the use of NEDAP voting machines in the communities of Stuttgart, Hannover, Arnsberg, Bonn, Dortmund, Köln, Langenfeld, Troisdorf, Bad Ems, Kastellaun, Mainz, Leipzig and Hamburg. In this meta-analysis, four dimensions were distinguished as common elements in all surveys:

1. Guarantee of a secret ballot;

    a. Is the ballot secret
    b. Are the voting machines reliable
    c. What is the liability for technical errors

2. Comparison of the voting machine with the traditional paper ballot method;

3. Assessment of the user friendliness; and

4. Overall judgment.

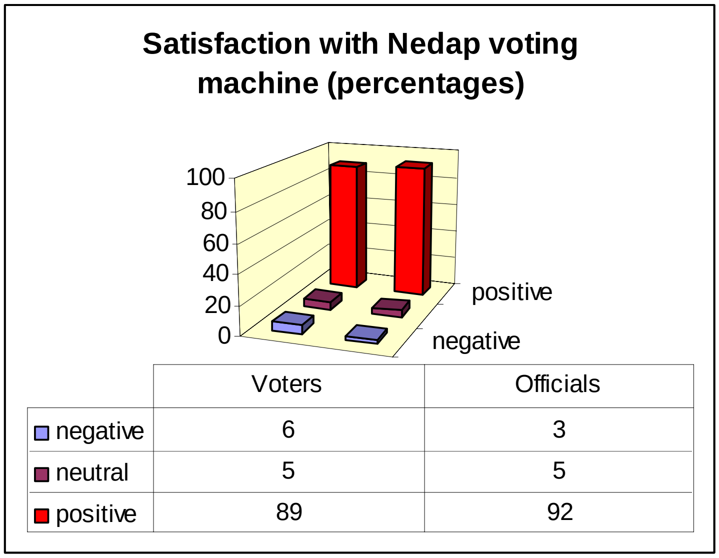
All together, the citizens of the 13 communities had a very high acceptance as well as a positive overall judgment as well. In particular, older and female voters scored very high on the four dimensions. The election officials were also very positive, especially about the decrease in the number of invalid votes; about the quick end-results and about the lower costs.

The University's own research surveyed 1182 voters, using the same design with the four dimensions. Summarising the results, it turned out that there was very little skepticism towards the anonymity; that almost everyone qualified the use of the voting machine as 'simple' and 'not difficult'; that the respondents were satisfied with the information they received about using the machines (before and during the voting) and there were hardly any suggestions for improvements and that the overall judgment was very positive, especially from the older and female voters.

The survey results from the election officials' yielded comparable results (see figure 2).

[20] Prof. Dr. U. Sarcinelli und Nina Thomsen, M.A. Einsatz elektronischer Stimmenzahlgeräte bei der Wahl zum vierzehnten Landtag Rheinland-Pfalz am 25.03.01. Studie im Auftrag des rheinland-pfälzischen Ministerium des Innern und Sport. Universität Koblenz-Landau. September 2001.

Figure 2: Satisfaction with NEDAP voting machines (%)



	Voters	Officials
🟦 negative	6	3
🟪 neutral	5	5
🟥 positive	89	92

The representative of NEDAP in Germany added some other positive results of the use of voting machines: the reduction in the number of polling stations and polling station personnel and fewer blank votes[21]. Based on the experiences in Germany and The Netherlands, NEDAP claims a decline in the number of polling stations of 20 – 25 per cent.

Looking at the official statistics for Cologne, Dortmund and Neuss, the reduction in polling stations and personnel is even larger.

		Past		Present		
	Electorate	polling stations	personnel	polling stations	personnel	reduction personnel %
Köln	711.000	800	5.600	540	2.700	53
Dortmund	430.000	478	3.346	280	1.400	42
Neuss	113.966	126	882	96	480	54

Source: Wahlamt Köln and HSG Wahlsysteme GmbH, Werne.

The following sections discuss the experiences of the City of Cologne with the use of NEDAP machines. This part is based on two interviews with members of the staff of the Election Bureau (Wahlamt Köln) and on a review of a number of articles and relevant press clippings.[22]

The City of Cologne has used voting machines since 1999 and between 1999 and 2004, 7 elections took place: Europawahl in 1999, Kommunalwahl and Oberbürgermeisterstichwahl (2x) in 1999, Landtagswahl in 2000, Stichwahl Oberbürgermeister in 2001 and Bundestagswahl in 2002. Experiences with the voting machines have been positive. On average 600 machines were used and

[21] Eine Kette von Vorteilspunkte. HSG Wahlsysteme GmbH, Werne (www.wahlsysteme.de)

[22] E-mail 24 March 2004 drafted by Mr. Michael Friedrichsen (Head of the Central Election Office Köln) and Mr. Stefan Grewing.

only in 11 cases were there small technical problems. The election officials submitted only positive reports and because the activities are less complicated and time consuming, the number of polling stations could be reduced from 800 to 540 and the number of personnel per polling station declined from 7 to 5. The Physikalisch-technischen Bundesamt tested the voting machines including the embedded software. The counting and tabulation software, however, was not part of the PTB testing. Furthermore there were no security problems; neither was there any errors observed in the counting of the votes.
The voters of Cologne also judged the switch to electronic voting machines positively: a survey held in 2001 showed that only 1.9 per cent were of the opinion that the voting process was now more complicated than it used to be, while 6.4 per cent saw no improvement.[23]

5 Final remarks

The introduction and the use of voting machines in the Netherlands and in Germany can be characterised as uneventful. Although there were (and are) critics who point out that serious problems exist, in particular with the secret source code and the lack of a voter verified audit trail, the debates were rather marginal.

In the Netherlands, there was never a serious discussion in Parliament or in the councils of the 419 communities that use voting machines. The discussions initiated by scientists and journalists were never very heated and did not reach much prominence in the media. One can conclude therefore that, although some discussion will continue to take place and regulations and conditions will be adapted on a regular basis, the use of voting machines is widely accepted.

At present, the attention of politicians and the media is concentrated on the next phase: ‘distance voting’. The idea behind this is to make it easier for citizens to cast their vote by offering them more alternatives, like voting by telephone and Internet. On 11 December 2003, a law was published[24] concerning the regulation of a number of experiments in the realm of *distance voting*. In this law, several possible experiments are outlined. Within the context of this report we like to mention two of them.

1. A first experiment is to allow voters to choose the polling station they like; and
2. A second experiment concerns telephone and Internet voting for those who reside in another country and who, until now, can only vote by mail. The security problems involved in especially the latter mode of voting are manifold and far more complicated than those with voting machines. Discussions therefore concentrate on new issues such as voter identity, secrecy of the ballot and hackers.

Despite all this, it is expected that the Dutch Government will give the green light for setting up these experiments at the elections of the European Parliament in June 2004. It would appear nearly certain that these new e-voting developments will generate much more debate than the voting machines ever did.

[23] Leben in Köln – Umfrage 2001 (Kommunaler Mikrozensus). Amt für Stadtentwicklung und Statistik.
[24] Experimentenwet Kiezen of Afstand. Staatsblad 2003, nummer 569.

Appendix: List of persons interviewed

Interviews (telephone and/or face-to-face) were held with the following persons:

- Ir. Peter Knoppers, technical University Delft
- Mrs. Mr. Drs. E. Pronk (Elections Advisory Board: Ministry of the Interior)
- Mr. G.J. Boon (Elections Advisory Board: Ministry of the Interior)
- Mr. H.B.M. Steentjes s.t. (NEDAP)
- Mr. H. van Wijk s.t. (NEDAP)
- Mr. J. Groenendaal s.t. (Powervote)
- Mr. Koning s.t. (TNO Electronic Products & Services B.V.)
- Mr. M. Friedrichsen s.t. (Head Wahlamt Köln)
- Mr. S. Grewing s.t. (Wahlamt Köln)

References

- Algemene Maatregel van Bestuur, *Regeling voorwaarden en goedkeuring stemmachines 1997*. Ministerie van Binnelandse Zaken, 11 juli 1997.

- Barry, Colin et. al. *eVolution not Revolution. Electronic Voting*. Status report 2. September 2002.

- David Chaum. *Secret-Ballot Receipts and Transparent Integrity. Better and less-costly electronic voting at polling places*.

- Congress of the United States. *Letter of HAVA authors*, Washington DC. March 3, 2004.

- *Eine Kette von Vorteilspunkte*. HSG Wahlsysteme GmbH, Werne.

- *Experimentenwet Kiezen of Afstand*. Den Haag, Staatsblad 2003, nummer 569.

- *Goedkeuring Software Zetelverdeling*. Het Expertise Centrum, 2000.

- *Handleiding Integraal Stemsysteem voor Windows*. NEDAP/Groenendaal

- Hogan, Shane and Robert Cochran (2003), *Electronic voting in Ireland. A threat to Democracy?* Report prepared for the Labour Parliamentary Party.

- Jacobs, Bart (2003), *De computer de wet gesteld*. Oratie, Nijmegen.

- *Kiezen op afstand. Eindrapport*. Het Expertise Centrum, 2000.

- *Leben in Köln* – Umfrage 2001 (Kommunaler Mikrozensus). Amt für Stadtentwicklung und Statistik.

- McGaley, Margaret and Dr. J. Paul Gibson (2003), *Electronic Voting: A Safety Critical System*

- Mercuri, Rebecca (2002). *A Better Ballot Box?* IEEE Spectrum Online..

- Mercuri, Rebecca and Peter G. Neumann (2002), Secure Electronic Voting. In: Dimitris Gritzalis, ed. Advances in Information Security, Volume 7. Boston, Kluwer Academic Publishers.

- NEDAP Specials. *Functional specification NEDAP Voting System ESI2*, 2003.

- Neumann, Peter G (1993), *Security Criteria for Electronic Voting*. Paper presented at the 16th National Computer Security Conference Baltimore, Maryland, September 20-23 1993.

- Pieters, Wolter (2003), *Stemmachines in Nederland*. Security of Systems Group; Katholieke Universiteit Nijmegen

- Richter, Prof. Dr. Dieter (PTB). Lehren aus der Wahlgeräteprüfung für Online-Wahlen. Erweiterte Fassung des Kurzvortrages anlässlich der Workshops „Online-Wahlen“ beim Bundesministerium der Innern, Berlin, 11 December 2001, erarbeitet unter Mitwirkung von Herrn Dr. Volker Hartmann und unter Verwendung von Materialen von Herrn Dr. Norbert Greif, beide PTB.

- Sarcinelli, Prof. Dr. U. und Nina Thomsen, M.A (2001), *Einsatz elektronischer Stimmenzahlgeräte bei der Wahl zum vierzehnten Landtag Rheinland-Pfalz am 25.03.01*. Studie im Auftrag des rheinland-pfälzischen Ministerium des Innern und Sport. Universität Koblenz-Landau.

- Stand van zaken automatisering rond verkiezingsproces. Het Expertise Centrum, 1999.

- *Test report concerning the compliance of a voting machine for use at elections in Ireland, Brand NEDAP, Model ESI2, with parts of the standard IEC 60839-I-3. TNO,* 2003.

- Wadsworth, Joe and Brian Wichmann (2003), *Report on Irish STV Software Testing*.