Technical Audit of an Electronic Polling Station: A Case Study

Hector Alaiz-Moreton, Universidad de Leon, Spain

Luis Panizo-Alonso, Universidad de Leon, Spain

Ramón A. Fernandez-Diaz, Universidad de Leon, Spain

Javier Alfonso-Cendon, Universidad de Leon, Spain

ABSTRACT

This paper shows the lack of standard procedures to audit e-voting systems and also describes a practical process of auditing an e-voting experience based on a Direct-recording Electronic system (D.R.E). This system has been tested in a real situation, in the city council of Coahuila, Mexico, in November 2008. During the auditing, several things were kept in mind, in particular those critical in complex contexts, as democratic election processes are. The auditing process is divided into three main complementary stages: analysis of voting protocol, analysis of polling station hardware elements, and analysis of the software involved. Each stage contains several items which have to be analyzed at low level with the aim to detect and resolve possible security problems.

Keywords: *Audit Process, Direct-Recording Electric Systems, Electronic Polling Station, E-Voting, Security*

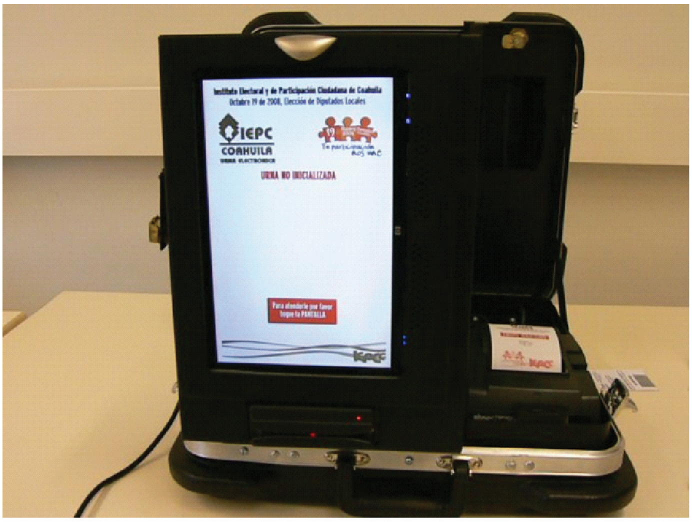
Elections are the most important processes in a democratic country; as citizens must accept not only the results but also whole process. Hence, only if both, security and the transparency are guaranteed, e-voting systems will be acceptable tools in the elections processes.

There are two types of electronic voting systems (Puiggali, 2007) remote e-voting.and face e-voting. Main difference between these kinds of methods is the physical situation of the elector. In the first one the user uses TCP/IP support to vote. In the second one, the user goes to his electoral district to vote and make his election, aided for a digital voting system (Ruth & Mercer, 2007). This system is called polling station based on D.R.E (Direct-recording Electronic). D.R.E. station saves the vote of the users. When the Election Day finishes, results can be obtained soon with little effort.

The three common pillars of any election process are: confidentiality, integrity and availability (Morales, 20099). E-voting systems must, therefore, fulfill these fundamental pillars as any other traditional voting system. These

DOI: 10.4018/jesma.2011070102

Figure 1. Polling station (© Observatorio Voto Electrónico)



three pillars are implicit the main requisites of a D.R.E. system (Fujioka, Okamoto, & Ohta, 1992; Indrajit, Indrakshi, & Natarajan, 2001):

1. There is a secure authentication method to access the system.
2. Only the people authorized to vote can do it.
3. The anonymity of the voter and the privacy of its vote are guaranteed and preventing from any kind of coerciveness.
4. There exists some protocol that allows the authorities to test, verify and certify the system.
5. The system must be useful, easy to use and accessible to people with disabilities.
6. Intruders must be detected and potential attacks prevented.
7. The system must be robust, fault tolerant and available during the whole Election Day.
8. The whole process must be auditable.

It might appear that auditing a simple machine for counting votes would be an easy task, but nothing could be further from the truth. A technical audit of an electronic polling system, does not only need to check every single component but also must inspire confidence in potential users (Helbach & Schwenk, 2007). It should be an open process, clear and based on fixed standards. In practice this is dependent upon the laws and electoral authorities in the various countries and states involved. This leads to extensive and complicated debates. Some scholars even talk of the impossibility of performing a successful audit of an electoral procedure based on technology or propose a number of methods for indirect verification (Schoenmakers, 2000).

This paper describes a real audit of a real electronic voting machine, Figure 1. It is the system of the State of Coahuila in Mexico, which has been used on a whole range of occasions since 2004 and recently in binding electoral processes.

The first difficulty was that of establishing the list of items to carry out the requirements described. In fact, there is no clear and comprehensive documentation on which to rely. In the section “Relation between secure items and requirements of the audit process” it can see like this list of items has impact on the eight requirements defined.

Every country, state and even electoral district has its own opinions on the topic. There are few published standards to act as a basis, and even when they exist, it is not always clear how to use them (Barrat, 2008). In the case of Europe there are certain recommendations made by the Council of Minister of the Council of Europe, designated Rec (Electronic Frontier Finland, 2008), but certain E.U. countries quite definitely do not observe them (Cohen, 2005). In the U.S.A. there are some developed proposal for standardization, thanks to the larger number of experiments, even successful, that have taken place there (Fischer & Coleman, 2006).

It was a big mistake on the part of the system and program developers and researchers to assume that the level of security for electronic voting would be similar to what is needed by financial institutions (Cox & Rubin, 2004). For the latter, the confidential operation may be made known to authorized third parties, while, in contrast, in electronic voting anonymity is an essential part of the process. Hence, nobody can be permitted to obtain information about how anybody votes other than in the final count, and then only for the purpose of totalling the votes cast. These kinds of drawback demand the use of a range of techniques for indirect checking of votes, such as V.V.A.T., or voter-verified audit trial (Mercury, 2007), which complicates and slows down the use of machines involved in electronic voting. Despite everything, there are obvious limitations on the security of this equipment unless appropriate measures are taken from the very start of the process of designing it (Armen & Morelli, 2005; Kohno, Stubblefield, Wallacj, & Rubin, 2004).

Another negative aspect is the apparent ease with which it would be possible to perpetrate fraud with D.R.E. polling system. In the present case, there are rigorous studies (Di Franco, Petro, Shear, & Vladimirov, 2004), that demonstrate that minor tinkering with the master copy of the voting software would be enough to allow electoral fraud on a grand scale. Moreover, a considerable part of the electronic voting systems market is in the hands of private companies that are reticent about opening up their systems to audit by third parties (McGaley & McCarthy, 2004). All of this means that extreme precautions must be taken during the audit process, which must leave no aspect of the security of the device and its software unchecked. There are other sorts of audit to cover features of the accessibility and usability of electronic voting equipment (Falcão, Cunha, Leitão, Faria, Pimenta, & Carravilla, 2006).

Other examples of e-voting experiences, which have been cancelled due to the fact that the audit process had not been well defined, are Netherlands, and Ireland, where the Independent Commission on Electronic Voting (I.C.T.E.) decided not to use the D.R.E due to lack of one organization and one standard dedicated to ensured the correct work of the electronics polling systems (Commission on Electronic Voting, 2010). On the other hand, Brazil, where the vote of the citizens is compulsory, the D.R.E. system based on biometric security primitives, are being very accepted thanks to voting specifications defined by Brazil’s Superior Electoral Tribunal (TSE).

In countries such as Spain (Gutiérrez-Rubí, 2009) or United Kingdom (Open Rights Group, 2007), several experimental experiences have been done with not binding results; due to laws of country do not permit e-voting systems in official government elections. However some binding e-voting processes have been used in private companies such as football clubs or banks (Real Madrid, 2009).

There are many manufactures of D.R.E. systems such as INDRA (Electoral Advisory Systems for Citizens, 2004; Indra, 2009), Bharat Electronics Limited, (Bharat Electronics, 2009), Hart InterCivic (Ladendorf, 2008), Microvote General Corporation (2008), to mention only the most important. These manufactures develop polling station with custom software highly secure but not easy to audit in a standard process.

Other manufactures like Premier Elections Solutions have suffered several audit processes to analyze and study their security features (Feldman, Halderman, & Felten, 2007; Wertheimer, 2004; Lamone, 2003; Kohno, Stubblefield, Wallacj, & Rubin, 2004). Thanks to these audit processes each manufacture includes new features in its systems to insure the security and make easier the own audit process, however a critical question appears. Which is the standard audit process procedure? And more important, which is the standard where the security elements to be evaluated are collected?

In this context, the decision of using former experience was taken in order to draw up a document listing the basic requirements that had to be checked in the I.E.P.C.C.'s voting machine prior to undertaking the actual audit. This paper does not present results, since they are copyrighted by the I.E.P.C.C. and, therefore, subjected to confidentiality clauses, at least until they are officially published. For this reason, only generic security aspects of the audit are detailed, whilst the conclusions concerning the security of the audited system are avoided.

Case study: Electoral and Voter Participation Institute of the State of Coahuila

The Organizer of the Elections is the "Instituto Electoral y de Participación Ciudadana de Coahuila" (IEPC, 2008), an independent organization that also constitutes electoral authority.

The Electronic Voting Observation Unit of the University of Leon in Spain (OVE, 2005) has for five years been working from an academic angle in the field of technology-based voting and voter participation. It was chosen by the Electoral and Voter Participation Institute of the State of Coahuila (IEPC, 2008) to resolve the problems of auditing its model of voting machine, which was designed and developed by the Institute itself.

Election Process

For each electronic polling station, an electoral table supervises the voting process, including both, the casting of the ballots and the counting of the votes. Citizens who live in the constituency where the polling station is installed compose the electoral table. That means that a President, a Technical Secretary, a person in charge of counting, and a Substitute to replace any of the other three in case of absence.

The people of the Electoral Table have to do several tasks such as: open and close the Electoral Table, install, open and close the polling station, use the control codes, receive the votes, close the voting, close the polling station, count the votes, send the results and finally publishing the results at the Electoral College. All steeps have perfectly defined by the Electoral and Voter Participation Institute of the State of Coahuila.

The polling station of our case study is based on a printed code to operate the e-Polling Station. Two kinds of codes are available to operate the e-polling station: control codes and access election codes. In our station, these codes consist of printed barcode cards that slide through a reader. These codes allow the handling of the station, and must be used only by the president of the electoral table:

- Verification Code: To check the right function of the station prior to opening it.
- Open Code: Used just once each Election Day to start the voting.
- Close Code: To be used only once in order to finish the voting.
- Restore Code: In case of power failure, the station must be restarted and data recovered by means of this code.
- Reprint Code: To get a second copy of the printed ballot in case of malfunction during its printing.

Electoral Day: Opening

The Electoral Day, under the supervision of both, representatives of the political parties and electoral observers, the people of the electoral table will handle the polling station and guide all the process of casting the votes.

First, they will set the e-polling station up, checking also that the ballot box is empty. After that, they will count and register the number of available access codes so that they can certify, at the end of the day that the results from the e-polling station are valid. The president will install the station and the screen in order to guarantee the secrecy of the votes.

After installing the station, the president will open the station and check its function by sliding its verification code card. Once this task is finished, the Open Code will be used to open the station. The result of this operation is a printed report that must show that the database is empty and, therefore, no votes at all. The number of access votes is also printed, and must match the number of cards received. Finally, date and hour of opening are also printed. This printed report must be attached to the minutes taken during the whole Election Day.

In case of failure of the electronic polling station, the ballots will be cast with a traditional ballot box, being this fact written in the minutes (and also in the incident registration form). After this previous work, the president will open the Electoral College.

Changing the Station's Address

Each electronic Polling Station has to be placed in the address the Electoral Authority decides. It can only be changed due to the following reasons: The selected place does not exist; it is closed; it is a forbidden place (a factory, a church, a bar, etc.); it does not allow the privacy, secrecy of the vote; there are no easy ways to access it; in case of force majeure. The new location must be placed in the same constituency and as close as possible to the original one, being its address published in the outside of that original location.

Reception of the Votes

Each voter will show his/her credential to the president, the technical secretary will check that his/her name appears in the Electoral Register and, eventually, the president will give the voter its access code. The voter will go to the station, touch the display and follow the audiovisual instructions that will appear. After a vote is cast, a ballot is printed in order the voter to check it and cast it in a traditional box.

If a ballot is not properly printed, the president will use de reprint code to allow the voter to get a new copy of the ballot. The reprint code will also be used after changing the printer paper roll, in case it would be necessary.

The Opinion of the Users

During the design of the audit process two simulated voting experiences were carried out to know the opinion of the users about electronic voting systems.

The first experience was based on a fictitious election process. A set of users used the polling station to select their favourite's icons to represent an unreal company. After that, users filled up a questionnaire, extracting the following conclusions (score from 1 to 5):

- Information about operation system: 3,884
- Confidence in the voting system: 3,186
- Security of election: 3,186
- Simplicity in the voting procedure: 3,163
- Speed of the voting process: 4,8

Analyzing results it can be say that DRE system is a good way to develop an election process, thank to its speed and the generous package of information showed along election process. However features such as usability and the perception of safety should be improved.

Other important fact is that the 64% of the respondents preferred the e-voting than traditional procedure, according with this quantitative data, is necessary to ask itself, how to convince the other 36 percent. The answer is: "improving perception of safety".

The final score of the election process developed with an electronic polling was 8.3 over 10 a good calcification but have to be improved the perfection of safety feature if a country want to use e-voting system in an official election process.

The second experience was developed in TECNOMEDIA (2009), a technologic fair. Thanks to special setup of the polling station, users filled up a questionnaire using the polling station to select each option of the questionnaires with the following result:

- 43% of the users would use this system if previously a security audit process is made.
- 27% of the users would use this system in any case.
- 14% of the users would use this system to no official elections; this is in not binding democratic processes.
- 10% of the users never use this system.
- 6% of users do not have an explicit opinion.

One more time the perception of safety is a big handicap due to a high percent of users prefers a DRE system audited due to they see a polling station like a black box.

Scenario of the Testing Experiences

First experience was developed in the University of Leon. The number of participants was 172, divided in different groups of students: fourth course of biology science, second course of mining engineering and a course of a special program of the University of Leon oriented to people with more 65 years old who want to study and to acquire generic knowledge in new technologies.

Second experience was developed in a regional fair called TECNOMEDIA 09, which main goal is the divulgation of new technologies. The number of participants in the experience was 210. The users profile was very heterogeneous, from young students of primary schools, to computer science professionals and people without knowledge in informatics.

DESIGN OF THE AUDIT PROCEDURE

The audit procedure presented in this document was divided into a series of stages. This was done in order to simplify the tasks that had to be performed and thus set up, an optimally efficient auditing method that would guarantee security and viability of the electronic voting system under real-life conditions.

It is worthwhile emphasizing that the group of assessable components that will be outlined are those which for one reason or another proved to have some weak point during the experiences of electronic voting that are covered by this paper. The analysis of these components can be extrapolated to experimental uses of other different electronic voting systems. It will serve as a complement to future auditing processes in such as way as to define a generic procedure applicable to any system.

The division of the auditing procedure into three groups of features for analysis was intended to facilitate the task of listing and assessing all the components involved in an electronic voting system. These three groups of features may be summarized as comprising study of the following:

- The protocol for voting by means of electronic polling systems (electronic voting machines or ballot boxes).
- The hardware components of the electronic voting machine.
- The software components involved in the voting process.

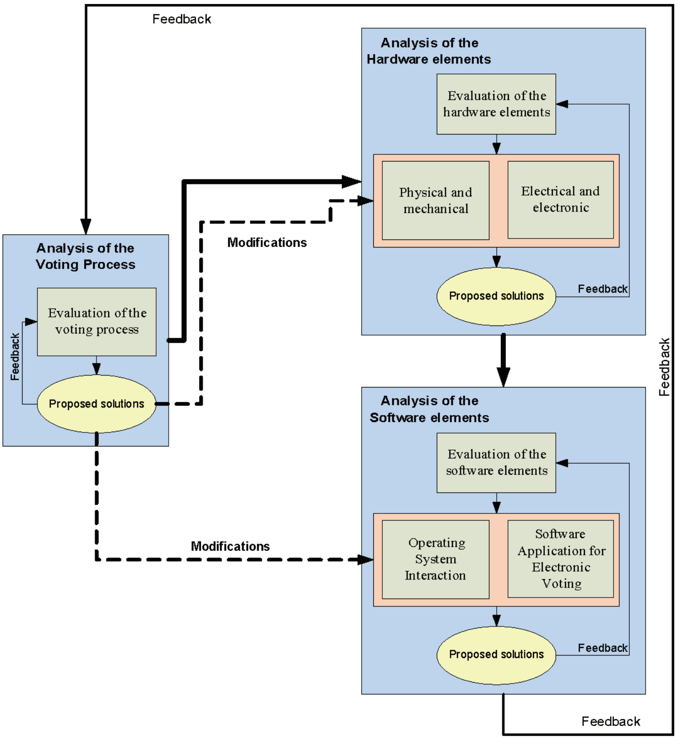
The reason that the first set of features to be studied are those included in the voting protocol is the fact that certain weak points in this might in some instances be remedied. This would be by means of changes and improvements to the hardware and software components, which would logically follow proposals for solutions relating to the voting protocol. Figure 2 shows the auditor process with its three stages associated and how solutions proposed after the first stage (analysis of the voting process) may involve modifying hardware and software elements).

As occurs on the ISO standard safety, items discussed in the audit process designed will be described at low level and although these items might seem trivial, is necessary to revise all of them to guarantee the polling station security.

Analysis of the Voting Protocol

This section reviews a number of features involved in the voting procedure, some external,

Figure 2. Scheme of the audit procedure (© Observatorio Voto Electrónico)


Feedback
Analysis of the Hardware elements
Evaluation of the hardware elements
Physical and mechanical
Electrical and electronic
Proposed solutions
Feedback
Modifications
Analysis of the Voting Process
Evaluation of the voting process
Feedback
Proposed solutions
Feedback
Analysis of the Software elements
Evaluation of the software elements
Modifications
Operating System Interaction
Software Application for Electronic Voting
Proposed solutions
Feedback
Feedback

some internal. An attempt has been made to pre-empt the problems of security and efficiency which are critical in a context as complex as that of electronic voting.

Hence, an assessment was made of a range of aspects involving logistics, environment and protocols that will define the quality and security of the process of voting. The various elements intrinsic to the voting process are considered in depth below. A description of what is evaluated and the requirements that should be met is given in each case.

User operations. The officials assigned to a given polling station should not carry out any action individually. This would ensure that all actions involving validation, resetting, closing or opening will not be undertaken by only a single user. To avoid this risk, users with personal secret PINs (Personal Identification Number) must be added.

Procedure for initializing and powering down machines. In no circumstances should it be possible during the polling process to turn an electronic voting machine on or off, other than in such a way that all the registers or meters recording the results of voting are re-initialized to zero. Software of the polling station must be supported this types of operations whether controlled or not.

Administrator access to voting machines. It should be impossible to duplicate items giving access to the electronic voting machines, such as cards with magnetic stripes or printed bar codes. This requirement is intended to ensure that no undesirable person will be able to undertake actions that would affect the electoral process. The best way to avoid this risk is to use personal smarts cards with a password associated.

Security of the physical space. There should be a physical space in which each electronic voting machine can be under constant visual surveillance so as to ensure its physical integrity and thus avoid sabotage. This requirement should be subject to compatibility with the need for privacy when voting. Public and private security officers are responsible of this task.

Environmental security. It should be made certain that the positioning of voting machines is such that they will not be exposed to external risks such as those arising from weather phenomena. To minimize this risk, the vote process should be developed in institutional buildings.

Maintenance and support. The voting machines should have a capacity to remain operational during the entire period of voting, from the start of polling until the downloading of data to allow compilation of the results. A technical expert has be stay in the Electoral College to solve any problem.

Availability of languages. The voting machines should be able to handle a range of languages or dialects. This is a software developed task.

Analysis of the Hardware Components of Machines

In order to cover all the components in the electronic voting system, these were grouped into two categories. On the one hand, there were the physical and mechanical components, on the other the electrical and electronic components.

Physical and Mechanical Components

This section refers both to those components which are intended to ensure the physical integrity of the electronic voting system and to those elements which are intended to make its use, accessibility, handling and transport easier.

Seals. There is a need for a system of seals that would reveal any potential undesirable tampering. This should be able to cover all the stages from transporting the voting machine to the polling station up to the point when results are reviewed and validated. This item must be studied in the physical design stage of the polling station by the manufacture.

Locks. A set of high-quality locks should be fitted to those parts of a voting machine which need to be accessible for carrying out repair or maintenance operations on the polling day. Manufactured is the responsible of the quality of these items.

Ventilation systems and operating temperature. The temperature inside the machine where its central processing unit is sited must remain in the acceptable range for the correct operation of the system. This problem can be solved by a low power fan.

Physical accessibility. The system must have appropriate arrangements to allow adjustments to the position of the voting machine. This is in order that electors with any sort of handicap can still get access to it so as to cast their votes.

Mobility. The system should be easily transportable to polling stations. For this purpose, various factors should be taken into account, such as the system's total weight, its ruggedness of construction and the ease with which it can be handled when being moved.

Confidentiality. There must be appropriate physical components to ensure the confidentiality of voting. To avoid this risk is very important the correct situation of the polling station in the Election Day.

Enclosure. The physical structures within which the computer system is enclosed must be such as to protect it against potential sabotage. Thus, all hardware devices incorporated in the electronic voting machine that are not directly involved in the action of casting a vote must be totally out of reach to any user other than repair and maintenance staff.

Electrical and Electronic Components

This section assesses the features relating to components such as computer equipment, systems providing electric current (power supplies, protection, cabling) and peripheral devices

Power supply surge protection. There should be systems to protect against surges caused by variations in the mains electricity supply that might damage the equipment. A UPS (Uninterruptible Power Supply) is highly recommended.

Cabling. The set of cables supplying power to the various devices should be totally hidden. If, for good cause, this is not possible, they must be shielded from any possible tampering by some protective fixture. Manufactures must take into account this problem in the design process of DRE system.

Identity document reader. The system for reading the identity documents that allow to voters access should be robust enough to prevent impersonation by duplicating voter credentials. The best solution is to utilize reusable smart cards and a reader for these to discard the printed credentials, illegally copied.

Battery life. The capacity of the batteries feeding the electronic polling system must be sufficient to keep the electronic voting machine operational throughout the polling period, even in the case of a power cut. With this in mind, consideration should be given to installing an uninterruptable power supply, to the use of high-capacity batteries and to attempting to incorporate low-drain devices. If the polling station is a based on a tablet-pc or laptop, the battery should have a minimum of six cells. If the polling station is based in a simple PC system is recommended the use of an UPS (Uninterruptible Power Supply) system.

Heat sinks. The system must have fitments that will dissipate heat in those places where an overheating problem could occur. Furthermore, all unnecessary mechanical parts should be eliminated in order to avoid increased power consumption by the system, which would lead to greater heating, as well as a reduced ability to run independently of a mains power supply.

Printer electricity supply. The printing devices must have a power supply independent from that of the computer system. This is so that it can print the voting docket necessary for the audited voting arrangements. One more time, using an UPS (Uninterruptible Power Supply) is much recommended.

Wireless interfaces. Access to wireless interfaces of types such as Bluetooth, IrDa, the WiFi 802.11 family and Wimax should be physically restricted. The aim of this is to ward off malicious attacks such as buffer overflows or the feeding of malicious code into the system. Wireless interfaces locked are an action that should be done by software and hardware mechanism.

Input and output devices. Access to laser disk drives and U.S.B. interfaces should be physically restricted, with the same intention as mentioned in the previous paragraph.

Hard disk storage. Measures should be in place to avoid the loss of data filed on internal storage units. This assessment looks at measures such as the implementation of some level of redundant arrays of independent disks (RAID), or storage based on solid-state memory, which is more stable and consumes less power than conventional hard disks.

Analysis of Software Components

The sections below cover the logical elements going to make up the electronic polling system. They refer to those aspects relating to the software application for voting and the operating system under which this application runs.

Interaction with the Operating System

The operating system is a key item when it comes to determining the overall security of the polling system. Good administration of the operating system is crucial in ensuring the proper functioning of the electronic polling system as a whole, since it controls the hardware peripherals and the software applications for voting.

Restriction of access to the operating system. Execution of the applications program that enables voting must be in full-screen mode, not allowing any interaction with the operating system under which the application runs, particularly at critical points such as an unexpected rebooting of the system.

User management. There should be a hierarchy of users with the following structure:

- Elector: a person using a voter identity document to cast a vote.
- Polling officer: any of the users who are responsible for the actions involved in managing voting machines during polling.
- Administrator: a user who sets up and configures the voting machine. Nomination of this person should be the responsibility of the manufacturer.

In this way a second line of defense is established if the requirements expressed in the previous section are not properly fulfilled.

Log files. There must be a set of mechanisms to record the actions carried out on the system, with the intention of certifying that the electronic polling has functioned correctly. These mechanisms must ensure checking and logging of:

- Signing on and off by each of the various groups of users.
- Exceptions and faults.
- The actions performed by each generic elector user, always with the caveat that voting confidentiality should be maintained.
- Monitoring of the processes of start-up and close-down of the voting machine.
- All this information must be stored in an encrypted form. It should allow a security audit procedure to be performed if there is any suspicion that undesirable activities have been taking place.

System files. The operating system should ensure some form of security back-up copy is made so as to protect the data involved in the voting process.

Software Applications for Electronic Voting

These items are responsibility of the software manufacture. These enterprises have to apply specific quality controls oriented to general purpose software. Thanks to these controls the proper functioning is insured as well as the user interfaces adequacy.

The paragraphs below present those aspects that were analysed that refer to the quality and security of the software devoted to the voting process covered by this document.

Comments and documentation. The source code should include the comments and formal documentation necessary for incorporating improvements and thus giving a capacity for scaling up the system.

Graphic interface display. Care should be taken that the resolution of the screen on which the software runs can be adjusted to any format required.

Programming language. The language used to implement the application must allow for adaptation to new platforms in an efficient and secure way.

Software structures. The structure of the software should be adapted to new object-oriented methodologies and hence facilitate scaling up by means of improvements affecting different modules separately.

User interface. A user-friendly graphic interface should be provided in which the sequence of steps to be taken in order to cast a vote should be clear and concise. Each step in the procedure should be accompanied by an audible explanation.

The set of items covered above refer to aspects concerning quality that must be kept in mind when the software is being written. Below, a definition is given of several major aspects that should be taken into account so as to ensure the security of the software.

Access to management codes. The set of codes needed to perform voting machine management actions should be protected, encrypted and outside the execution environment of the software application.

Access to elector codes. The voter codes associated with each identity document should be protected in the same way as the management codes, as in the previous paragraph.

Constituency configurations. It should be ensured that each electronic voting machine does not contain all possible configurations for all the constituencies in which it might be used. Each machine should be configured only for a single constituency, depending exclusively upon the initialization code. This aspect is critical because all the voting machines are identical, each one being "personalized" in accordance with the initialization code. The code in question is visible on the machine, and hence may easily be duplicated. In this way, it would be possible to produce multiple machines for one and the same place that would generate valid results but with different final outcomes.

Protection of electoral information. There must be some means for protecting the electoral information stored within the machine. This may be achieved either by means of the application and management of read and write permissions, or through some encryption protocol.

Diagnostics. Logs should be kept by the software application so as to ensure that the program is being executed and is functioning without any unforeseen events.

Information on progress. The is a need to present information such as which constituency a machine is assigned to, what maximum number of electors it permits, how many votes have been cast on it, among other relevant data, so as to permit a process of dynamic auditing to be carried out while voting is still going on. This information, together with the diagnostic logs mentioned in the previous paragraph and in paragraph, will ensure the consistency of the information referring to the process of voting.

Security of the electoral information within the machine. This point refers to the fact that the electoral software should guarantee that the information stored in the machine cannot be extracted by using particular software tools.

Security of communications between the machine and other devices. It should be clarified how the software will guarantee that other pieces of equipment do not communicate with it during polling and are not able to change the electoral information previously stored.

Security and authenticity of the machine's applications. The software and the process of production and configuration of the machine should guarantee that the software is authentic during all stages in the polling process.

Security of the secrecy of the ballot. It should be clear how the software guarantees that there is no way of identifying what choice each individual voter has made.

Relation Between Secure Items and Requirements of the Audit Process

The Table 1 shows how the items explained before affect in the eight requirements explained in the section "Technical audit of an electronic polling station: a case study".

Table 1. Items-requirements relation

	Requirements							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Items								
User operations	x	x	x	x	x	x		
Procedure for initializing and powering down machines							x	
Administrator access to voting machines	X	x		x				x
Security of the physical space	X	x	x				x	
Environmental security						x	X	
Maintenance and support								x
Availability of languages					x		X	
Seals					X	x	x	
Locks					X	x	x	
Ventilation systems and operating temperature							x	
Physical accessibility		x			x			
Mobility					x			
Confidentiality	X							
Enclosure					X		x	
Power supply surge protection							x	
Cabling							x	
Identity document reader	X	x		x				x
Battery life							x	
Heat sinks							x	
Printer electricity supply				x			x	x
Wireless interfaces		x				x	x	
Input and output devices		x				x	x	
Hard disk storage							x	x

continued on following page

Table 1. continued

Restriction of access to the operating system	X	x	x	x	x			
User management	X	x	x					X
Log files				x				x
System files							X	X
Comments and documentation								x
Graphic interface display					x			
Programming language								x
Software structures	X	x						
User interface					x			
Access to management codes	X	x	x					X
Access to elector codes	X	x	x					
Constituency configurations							x	
Protection of electoral information			x					
Diagnostics							x	
Information on progress				x			X	X
Security of the electoral information within the machine			X	x			x	
Security of communications between the machine and other devices		x					x	
Security and authenticity of the machine's applications							x	x
Security of the secrecy of the ballot	X						X	

Table 1 shows that the most important requirement is the number 7, "The system must be robust, fault tolerant and available during the whole election day" because the number of items influencing this, is quite big in comparison with others requirements. This requirement is strongly relational with the pillars integrity and availability.

It can observe that the rest of requirements are quite distributed along the list of items, this mean that all items are important to guarantee three pillars of e-voting and therefore the eight requirements defined.

CONCLUSION

Thanks to two testing experiences made before audit, it can be concluded that 43 percent of the users would use the electric polling station analysed in this work if and only if this system is audited by an external organization of experts in security, also can be concluded that the confidence level of the users is 8.3 over 10. Therefore is a main priority to improve the perception of safety, a big handicap if a country wants to utilize e-voting system to develop an official election process.

The outlined method is no more than a first step towards a definition of a document to serve as a basis for other technological audits of electronic voting machines due to the lack of formal auditing methods for this type of systems, where the application of ISO 27001, ISO 27002 and ISO 17799 is not possible, as these standards do not take into account specific aspects of systems designed for electronic voting purposes. Therefore the correct implementation of the items assessed defines the features of an accurate, secure polling system.

After applying the proposed methodology, and once its results are known, the system should be improved by interpreting the data and, hence, being applied again in order to refine the procedure.

Future work is, therefore, ensured with the aim of optimizing the methodology so that a standard can be proposed to set the security control items required for Direct-recording electronic voting systems.

ACKNOWLEDGMENT

We are very grateful to I.E.P.C.C. for its support.

REFERENCES

Armen, C., & Morelli, R. (2005). E-voting and computer science: Teaching about the risks of electronic voting technology. In *Proceedings of the Tenth Annual Conference on Innovation and Technology in Computer Science Education*, Bologna, Italy (pp. 227-231).

Barrat, J. (2008). Electronic voting certification procedures. Who should carry out the technical analysis? In Barrat, J. (Ed.), *E-voting: The last electoral revolution* (1st ed.). Ann Arbor, MI: ICPSR.

Bharat Electronics. (2009). *Electronic voting machines*. Retrieved from http://www.bel-india.com/index.aspx?q=&sectionid=237

Cohen, S. (2005). *Auditing technology for electronic voting machines*. Cambridge, MA: MIT Press.

Commission on Electronic Voting. (2010). *Independent commission on electronic voting and counting at elections*. Retrieved from http://www.cev.ie/

Cox, C., & Rubin, A. (2004). *Is the U.S. ready for electronic voting?* Retrieved from http://teacher.scholastic.com/scholasticnews/indepth/upfront

Di Franco, A., Petro, A., Shear, E., & Vladimirov, V. (2004). Small vote manipulations can swing elections. *Communications of the ACM*, *47*(10), 43–45. doi:10.1145/1022594.1022621

Electoral Advisory Systems for Citizens. (2004). *Indra*. Retrieved from http://94.126.241.45/webelecta/electa_indra_EN.htm

Electronic Frontier Finland. (2008). *Incompatibility of the Finnish e-voting system with the council of Europe e-voting recommendations*. Retrieved from http://www.effi.org/

Falcão, J., Cunha, M., Leitão, J., Faria, J., Pimenta, M., & Carravilla, A. (2006). A methodology for auditing e-voting processes and systems used at the elections for the Portuguese parliament. In R. Krimmer (Ed.), *Proceedings of the International Workshop on Electronic Voting in Europe: Technology, Law, Politics and Society* (LNI 86, pp. 145-154).

Feldman, A., Halderman, J., & Felten, E. (2007). Security analysis of the Diebold AccuVote-TS voting machine. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology* (p. 2).

Fischer, E., & Coleman, K. (2006). *The direct recording electronic voting machine (DRE)* (Tech. Rep. No. RL33190). Washington, DC: The Library of Congress.

Fujioka, A., Okamoto, T., & Ohta, K. (1992). A practical secret voting scheme for large scale elections. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology* (pp. 244-251).

Gutiérrez-Rubí, A. (2009). *El voto electrónico llega a España con las elecciones europea.* Retrieved from http://www.gutierrez-rubi.es/2009/06/04/el-voto-electronico-llega-a-espana-con-las-elecciones-europeas/

Helbach, J., & Schwenk, J. (2007). Secure Internet voting with code sheets. In A. Alkassar & M. Volkamer (Eds.), *Proceedings of the 1st International Conference on E-Voting and Identity* (LNCS 4896, pp. 166-177).

IEPC. (2008). *Memoria electoral: Electoral and voter participation institute of the State of Coahuila.* Retrieved from http://www.iepcc.org.mx/

Indra. (2009). *Indra realizará el escrutinio de las Elecciones al Parlamento Europeo del 7-J.* Retrieved from http://www.indra.es/servlet/ContentServer?pagename=IndraES/SalaPrensa_FA/DetalleEstructuraSalaPrensa&cid=1243482316640&pid=1087577300456&Language=es_ES

Indrajit, R., Indrakshi, R., & Natarajan, N. (2001). An anonymous electronic voting protocol for voting over the Internet. In *Proceedings of the Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems* (p. 188).

Kohno, T., Stubblefield, A., Wallacj, D., & Rubin, A. (2004). Analysis of an electronic voting system. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 27-40).

Ladendorf, K. (2008). *Casting its lot with e-voting.* Retrieved from http://www.hartic.com/news/77

Lamone, L. H. (2003). *State of Maryland Diebold AccuVote-TS voting system and processes*. Annapolis, MD: Maryland State Board of Elections.

McGaley, M., & McCarthy, J. (2004). Transparency and e-voting democratic vs. commercial interests. In R. Krimmer & Grimm, R. (Eds.), *Proceedings of the 1st International Workshop on Electronic Voting in Europe: Technology, Law, Politics and Society* (LNI 47, pp. 143-152).

Mercury, R. (2007). *Mercury's statement on electronic voting.* Retrieved from http://www.notable-software.com/RMstatement.html

Microvote General Corporation. (2008). *Election solutions.* Retrieved from http://www.microvote.com/products.htm

Morales, V. M. (2009). *Seguridad en los procesos de voto electrónico remoto: Registro, votación, consolidación de resultados y auditoria.* Unpublished doctoral dissertation, Universitat Politecnica de Catalunya, Barcelona, Spain.

Observatorio Voto Electrónico (OVE). (2005). *Electronic voting observation unit of the University of Leon.* Retrieved from http://www.votobit.org/ove/index.html

Puiggali, J. (2007). *Voto electrónico.* Paper presented at the 2nd Jornadas de Comercio Electrónico y Administración Electrónica, Saragossa, Spain.

Real Madrid. (2009). *El voto electrónico en la Asamblea.* Retrieved from http://www.realmadrid.com/cs/Satellite/es/1193040472656/1202766421991/noticia/Noticia/El_voto_electronico_en_la_Asamblea.htm

Ruth, S., & Mercer, D. (2007). Voting from the home or office? Don't hold your breath. *IEEE Internet Computing, 11*(4), 68–71. doi:10.1109/MIC.2007.94

Schoenmakers, B. (2000). Fully auditable electronic secret-ballot elections. *Internet Technology Magazine*, 5-11.

Wertheimer, M. (2004). *Trusted agent report: Diebold AccuVote-TS voting.* Columbia, MD: RABA Technologies.