Verification and Maintenance of e-Voting Systems and Standards

Paul Gibson[1] and Margaret McGaley[2]
[1]Le Département Logiciels-Réseaux, INT, Évry, France.
[2]Computer Science Department, NUI Maynooth, Ireland
paul.gibson@int-evry.fr
mmcgaley@cs.nuim.ie

Abstract: E-voting systems should be verified to be fit-for-purpose before being deployed, but there is a serious lack of provision for verification and maintenance in existing standards and recommendations for e-voting. A change to requirements, or to the system, usually results in the previously established fitness-for-purpose being compromised. Therefore change must be managed, and standards documents must make provision for their own maintenance.

Verification is a process of establishing a relationship between what is required of the system and properties of the actual system. It is good practice that an independent authority be responsible for verification of systems against requirements. It must be possible to determine whether a given authority can be trusted to fulfil this task competently. Thus, requirements documents must not only say what standards are to be met, but must also state the minimum capabilities expected of any testing authority.

The whole e-voting system development process is prone to human-error. This applies to the requirements, standards and the systems they describe. We must introduce suitable procedures for dealing with these errors, including the identification of responsible parties. We must also ensure that there is adequate incentive for the correction of errors. If maintenance of systems requires expensive recertification, there is a risk that vendors will not make necessary changes to their systems (to avoid recertification) or will make changes without having the systems recertified.

Error discovery is not the only agent of change for requirements and systems. For example, the introduction of new legislation, new election types, or new technology will have direct consequences. This requires careful co-ordination between all concerned parties. Whenever a system changes, whatever the surrounding circumstances, it must be tested and re-certified. However, if the system under evaluation has been well-engineered, it may not be necessary to begin again with every modification. In this paper we examine what it means for a system to be well-engineered and propose maintenance procedures specific to the problem of e-voting.

Keywords: Electronic voting, testing, certification, standards, maintenance

1. Introduction to e-Voting

In this paper, we examine issues concerning verification and maintenance of e-voting systems, their requirements and the standards that they are supposed to meet. Our arguments are generally based on the critical role of software in e-voting machines whilst acknowledging that e-voting is a systems engineering problem, rather than just a software engineering problem. All e-voting systems rely substantially on the correct functioning of their software. It has been argued that such e-voting software is critical to its users (McGaley and Gibson, 2003), and so one would expect to see the highest standards being applied in its development. However, where the software in e-voting machines has been open to examination it has often been demonstrated to be of very poor “quality”, even though it has previously been independently tested and accredited for use (Gibson, 2007).

Applying state-of-the-art computer and information technology to modernise the voting process has the potential to make improvements over the existing paper (or mechanical) systems; but it also introduces new concerns with respect to secrecy, accuracy and security (Gritzalis, 2003). The debate over the advantages and disadvantages of e-voting is not a new one, and use of such systems in actual elections has led to their analysis from a number of viewpoints: usability (Herrnson et al., 2005; Everett, 2007), risks and threats (Neumann, 1990), security and voting protocols (Groth, 2004), verification and validation (Cetinkaya and Cetinkaya, 2007) and codes and law (Mercuri and Camp, 2004).

The risks that have been clearly identified seem not to concern those responsible for procuring the systems. In fact, it appears that e-voting is just one well-publicised example of governments

wishing to adopt new technologies before the risks and benefits, as perceived by the public, have been properly analysed and debated (Horst et al., 2007).
In this paper we argue that poor maintenance procedures pose a major risk to the successful adoption of e-voting technology. Before deploying these machines, we should be able to trust them to do what they are supposed to do. In the future deployment of voting machines, maintenance becomes a real issue: when a previously trusted system is changed then should we continue to trust its behaviour?

2. Statement of the problem to be addressed

2.1 Verification

Verification is a process of establishing a relationship between what is required of the system and properties of the actual system. It is good practice that an independent authority be responsible for verification of systems against requirements. In the domain of e-voting this is normally done by an Independent Testing Authority (ITA). It must be possible to determine whether a given authority can be trusted to competently verify a given system against a given specification of requirements. Thus, requirements documents must not only say what standards are to be met, but must also state the minimum capabilities expected of any testing authority.

In an influential article, Kocher and Schneier (2004) state: “The threats are real, making openness and verifiability critical to election security.” In this paper we argue that verifiability is strongly dependent on maintainability: as a system evolves it needs to be maintained and continually verified against its requirements.

2.2 Requirements creep, evolution and maintenance

A major problem associated with any software system is that of requirements creep: the tendency for the set of requirements to continuously grow during the course of development, resulting in a system that is more expensive and complex than originally intended. Jones (1996) states: “One of the most chronic problems in software development is the fact that application requirements are almost never stable and fixed. … The root cause of requirements volatility is that many applications are attempting to automate domains that are only partly understood.” Requirements creep has been a major problem in e-voting systems. A good example is of the requirement for a voter verifiable audit trail. Many current e-voting machines do not meet this requirement, and were not designed to do so. However, the election administrators and manufacturers seem to believe that this additional functionality can be somehow bolted on to the machines without risk. Requirements creep is normally associated with changes to the system that are identified before the system is deployed for use. This is similar to requirements evolution where changes are requested to a system after deployment, and this leads to software maintenance, defined in IEEE Standard 1219 (IEEE, 1993) as: “The modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment”.

Gunter et al. (2000) emphasise the importance of considering the interface between the system and its environment when modeling requirements of any system. Changes in the environment (or our understanding of the environment) will have an impact on our requirements. It is clear that the political environment has been fundamentally changed by recent problems with voting technology and there is no reason to believe that this environment will stabilise in the near future.

A related problem is that the rapid change in technology leads to requests for new functionality (features). For example, paper voting usually results in a paper ballot being dropped in a secure urn with no way of later linking a vote to a particular voter. Thus, a voter cannot change their minds, remove their previous vote from the urn, and re-vote. With an electronic vote (and an electronic urn) there is no technical reason why such a re-vote cannot be facilitated. Technology could open up new possibilities to the users/voters resulting in pressure for new features to be incorporated in future versions of the system. However, this is not without serious risk: the addition of new features is a major problem in software engineering as there can be complex interactions that lead to incorrect behaviour that is difficult to find before systems are updated and deployed (Gibson, 1997).

2.3 Laws and standards: multiple layers, ambiguities, inconsistencies and integration

We must ask whether a given e-voting system is lawful, as a system which does not comply with international law should not be used in democratic elections. For example, the fundamental principles of elections are firmly stated in: article 25 of the *International Covenant on Civil and Political Rights* and article 21 of the *Universal Declaration of Human Rights*. Furthermore, voting systems are normally required to comply with laws at other levels of governance, for example: constitutional, national, state, regional, etc. Finally, many of these laws make reference to international and national standards that must be adhered to (or which act as guidelines to aid in the verification process).

An e-voting system has myriad inter-related legal requirements to meet; and it is not even clear whether it is possible for a given system to be considered lawful in such a complex context. Furthermore, these multiple layers provide very shaky foundations upon which to build a system – none of the layers are fixed and the texts are open to different interpretations. In many cases, one could argue that there is no consistent interpretation and that no system can be built that can meet conflicting requirements. When problems arise with a particular e-voting machine (or system) it is a complex, costly task for judges to decide if these were due to some aspect which could be said to be illegal.

The final problem to consider is that each voting system has to meet specific needs which are not directly addressed by the laws and standards. The requirements of the system must somehow integrate these specific needs with multiple layers of laws and standards. As changes are made to requirements within different layers, in parallel, then who is responsible for ensuring that the requirements can be re-integrated in a coherent manner?

As such changes are currently taking place throughout the world, the issues of maintenance and verification are sure to give rise to problems in the near future. For example, certain states in the USA have certified machines for use after a formal process of accreditation, but against a standards document which has subsequently been replaced (NYT, 2007). A consequence of this is that these machines need to be uncertified for re-accreditation against the newer, more demanding standards. However, if the manufacturers refuse to update their machines accordingly (or make excessive financial demands for doing so) then it is likely that such machines will become obsolete and the cost for their procurement will never be recovered.

3. Requirements specification and verification: The need for co-ordination

There are four main actors in the specification and use of e-voting system requirements:

- The standards bodies – establish the requirements that all e-voting systems (within a certain geopolitical space) must meet.
- The procurement offices – establish the requirements that a specific machine must meet in order for it to be purchased for use in a specific election.
- The manufacturers – develop machines that meet the generic requirements specified by the standards bodies and the specific requirements stipulated by procurement offices.
- The Independent Testing Authorities – test the delivered machines to ensure that they meet the requirements.

There are two main problematic scenarios that may arise within this structure. The first is that procurement offices may specify requirements that are inconsistent with those requested by standards bodies. We propose that it is the responsibility of the procurement office to put procedures in place to ensure that this does not happen. The second problematic scenario arises when a delivered system meets the requirements set by the standards bodies but not the requirements stipulated during procurement. In this case, the system could be certified as fit for purpose by an ITA whilst not being considered acceptable for use by the customers who procured it. We propose that it is the responsibility of the procurement office to set up suitable verification procedures to ensure that manufacturers develop and deliver products that meet their specific requirements, and to draft contracts in such a way as to ensure that this happens.

In the following subsections we argue that all four main actors have contributed to the current failure of e-voting machines to be trusted and to be worthy of trust.

3.1 International and national standards bodies

3.1.1 Council of Europe

The *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting* (CoE, 2004) was set up by the Council of Europe in early 2003 ". . . to develop an inter-governmentally agreed set of standards for e-enabled voting, that reflect member states differing circumstances, and can be expected to be followed by the ICT industry." (CoE, 2003)

The document they produced acknowledges that it cannot be judged in isolation. It states that it should respect: "the obligations and commitments as undertaken within existing international instruments and documents, such as [. . .]" The list of 12 instruments that follows - though it is clearly not meant to be exhaustive - covers a diverse range of documents, including the *Code of Good Practice in Electoral Matters* (Venice Commission, 2002).

This inter-related set of complex documents is analagous to a software system which has evolved over time, in response to ever changing sets of requirements. The system depends on a large number of other systems, and the environment of the system is not clearly understood. McGaley and Gibson (2006) propose a re-engineering of these standards, but note that this needs participation from a wide range of experts. However, there is currently no better alternative that could be adopted in place of the European standards; as Volkamer and McGaley (2007) state: "no requirements catalogue exists that expresses the requirements for e-voting systems with enough precision to be checkable".

3.1.2 Federal election commission (USA)

In the USA, multiple layers of federal, state, and local laws, policies, regulations, and procedures must be followed when running elections. The recount of votes in Florida during the 2000 presidential election exposed many problems with the traditional voting systems. To address these concerns, the Help America Vote Act (HAVA) was signed into law two years later. Currently, most election jurisdictions use systems that are required to conform to the 2002 standards developed by the Federal Election Commission (FEC, 2002). The standards present a certification procedure involving testing by an ITA and most jurisdictions are legally forbidden to use uncertified systems. Federal government is thus responsible for the testing, certification, decertification, and recertification of voting equipment. This responsibility has been assigned to the Election Assistance Commission (EAC), an independent commission established in 2003.

The American approach is much more prescriptive than that seen in Europe. However, there continue to be problems with deciding whether machines meet the standards or not. A main problem is that the standards documents are evolving quicker than the manufacturers are evolving their machines.

3.1.3 Standards maintenance is key

The fundamental problem is that the domain of voting is not well enough understood for us to currently develop a stable set of standards. This leaves one with a clear choice -

- Delay electronic voting adoption until a stable set of standards is produced, based on a scientific analysis of voting and the construction of a formal domain model, or
- Continue with the deployment of e-voting machines whilst: acknowledging that they currently do not meet requirements, developing procedures to mitigate the risk, and investing in the evolution and maintenance of standards.

3.2 Procurement offices

The Election Science Institute (ESI, 2006) of San Francisco, California was contracted to investigate why Cuyahoga County (Ohio) had so many problems with their voting system in the May 2006 election. The ESI Project Director, Steven Hertzberg, was particularly unhappy with procurement, stating: "Help America Vote Act has not stimulated sufficient competition among voting-equipment manufacturers…I don't want legislation to stipulate a solution, I want legislation to stipulate a set of requirements based on the needs of stakeholders. And then I want to be able to go out to private vendors and say, 'I need this. Build it.'"

In the American case, procurement offices were constrained by national legislation to purchasing machines from a small list of existing alternatives. In Europe this has not generally been the case, yet many procurement offices have made the same mistake of not fully understanding or modelling their requirements, in terms of the needs of the users, before procuring a system. The Irish case is typical; the independent Commission on Electronic Voting (CEV, 2006) wrote in their final report: "In the case of the chosen system, many of these requirements were largely predetermined by the fact that an existing design of electronic voting system was adopted and adapted for use in Ireland and that their existence was thus already implicit or explicit in that design."

Procurement offices around the world need more assistance in mastering the complexity of requirements engineering for e-voting. Ray Martinez, former vice chairman of the Election Assistance Commission which administered $3 billion in federal funding under the 2002 Help America Vote Act, summarised the problem by stating: "When you add so much complexity - federal mandates, state mandates, new equipment, statewide databases - to an endeavor so dependent on human interaction, you're bound to get mistakes."

3.3 Manufacturers

The manufacturers of the voting machines have the simple responsibility to act competently and professionally. They must develop systems in order to meet the specified requirements and attempt, to the best of their abilities, to verify the systems before they are submitted for independent testing. Manufacturers must be as transparent as possible with respect to the systems engineered and the processes followed in their development; otherwise, there is a real risk of a conflict between democratic and commercial interests (McGaley and McCarthy, 2004).

With respect to changing requirements, manufacturers must honestly declare when their products are unable to meet a requirement. With respect to testing, manufacturers must report all errors that have been found and how they have been corrected (if, at all). With respect to aiding the ITAs, they must endeavour to provide an audit trail between specific requirements and the components in their final systems (using design documentation to explicitly record important decisions), and to structure the system so that it can be maintained in a compositional manner.

3.4 Independent testing agencies

Though the European and American approaches to ITAs differ significantly, both have rightly come under close scrutiny.

Many European countries, including Ireland and the United Kingdom, have deployed e-voting machines that have been accredited by ITAs and then subsequently, as a result of public criticism, instigated their own independent analyses of the machines. Consequently, numerous published reports have identified fundamental flaws in the systems under test. There is bewilderment as to how these machines were deemed to be fit for purpose by the ITAs. Given that these agencies have demonstrated competence in other, similar domains, one must ask why the verification of e-voting systems against a standard set of requirements can lead to such an unsatisfactory conclusion. We argue that the poor specification of standards is largely responsible.

The European approach to accreditation (as adhering to a list of recommendations) is much less structured that that found in the United States – where the legal requirements are much more formally specified and have the potential to be strictly enforced. The American standards call for three levels of tests to be performed on voting systems to ensure that the end product is fit for purpose: *Qualification tests* to be performed by ITAs designated by the National Association of State Election Directors; *Certification tests* to be performed by the State; and *Acceptance tests* to be performed by the jurisdiction acquiring the system. Despite this logical, layered approach to verification, there have been many instances of certified election systems being "broken". Thus the question arises: if systems that meet the standards can be induced to provide inaccurate or unreliable results, is the problem that the standards are poor or is the problem that the verification processes are inadequate?

4. Maintenance

We propose that a change to the standards, requirements or system must result in a recertification of systems. A major risk with recertification is that a requested change to requirements cannot be implemented in time for recertification of the machines before their next use. A bigger risk is that the machines cannot be changed (with reasonable cost) in order to meet the new requirements.

4.1 Changing standards

One serious failing of many existing requirements catalogues for e-voting is the lack of provision for verification and maintenance. For instance, the Council of Europe requirements (CoE, 2004) call for "certification processes" without going into any detail about those processes. They make no mention of maintenance other than a brief note stating that they "may look again at this issue two years after the adoption [of these requirements]".

The development of a standards document should never be considered "complete" since technology is constantly changing, as is our understanding and expectation of that technology. Standards documents must make provision for their own maintenance in such a way that the verification based on them is not compromised. The standards under consideration themselves must be maintained, as vulnerabilities come to light, requirements change, and new technology becomes available.

The update of standards should not be done without the involvement of all stakeholders: the manufacturers (who are aware of future technological changes), the procurement officers (who are aware of changing requirements in their particular jurisdictions), the testing agencies (who will be required to verify systems against the standards), and a wide range of system engineering experts (including specialists in software and system maintenance).

We propose that standards be updated following a regular frequency such that machines are not expected to be updated more than once between elections. The precise frequency needs to be agreed as part of the standardisation process, and being able to maintain the machines to this frequency should be established through the accreditation process.

4.2 Changing requirements

As standards evolve, requirements for specific machines will usually have to be maintained (to guarantee consistency). However, we expect that specific requirements may need to change at a greater frequency than the standards. For example, improvements to the interface of a specific machine may be desirable (rather than legally required) and this change should not have to wait for the standards to be updated in order for it to be implemented. ITAs should not have to be recertified when requirements change. However, individual machines will certainly need re-certification.

4.3 Changing implementation (of the e-voting systems)

We note that the e-voting systems will normally have to change in response to changes to standards and requirements. However, a new requirement can often be met in one of three ways:

- Make no changes to the machine but change the procedures for using the machines.
- Make changes to the machine but no changes to the procedures.
- A combination of the above.

We note that making changes to the machines is a *high-risk* option where software is involved: a small change in one software component can result in undesirable behaviour in other software components.

E-voting systems, being man-made artefacts, are not expected to be perfect. Thus, we expect to have to manage a situation where a machine is shown to malfunction. In such a situation, there are two distinct possibilities:

- The machine is incorrect in the sense that it does not meet its requirements.

- The requirements were incorrect in the sense that they did not correctly express the needs of the customer.

In the first instance, we must change the implementation and recertify the machines. Furthermore, we must also investigate how the machines were incorrectly certified to be correct in the first place, and introduce maintenance mechanisms to ensure that this type of problem cannot happen again. In the second instance we must change the requirements documents (and, as is normally done, carry these changes through to the implementation of the e-voting system).

4.4 Managing error and risk in evolving requirements

Since the whole development process is in human hands, it is prone to human-error. This applies to both the requirements and the systems they describe. Errors will almost certainly be found (and will certainly exist) in the requirements themselves, and in design, implementation, testing and use of systems. Therefore we must design procedures for dealing with these errors, including identification of responsible parties. These procedures could not be carried out by one of the four agents (identified in section 3), for obvious reasons.

Timing is very important: if a grievous error is discovered between elections, there may be time to deal with it before the system must be used again. There may be much more serious consequences if it is discovered just before an election, or worse, just after an election has been completed. An independent agency must decide how serious a given error is, and how it should be dealt with in the short, medium and long term. Consequently, we recommend that there must be another agent introduced into the process of election administration.

The role of this fifth agent would be to supervise re-certification and re-accreditation. They would be responsible for deciding which system components need to be re-certified for use after a change to requirements, whether a change to standards meant that an ITA needed to be re-certified and which subset of functions of the ITA were concerned.

5. Conclusion

As the media continues to report on the “failure” of e-voting machines, electoral administrators and e-voting machine manufacturers have been required to review their policies and systems in order to meet a set of ever changing requirements. Such an unstable problem domain stretches their understanding of the electoral process and their ability to apply a diverse range of technologies in providing acceptable electronic solutions. The breadth and depth of the issues suggest that no electoral administration can justifiably claim to have implemented a “trustworthy” electronic replacement for a paper system.

Requirements capture is the first step in the process of meeting customer needs. The process is required to fulfil two very different needs: the procurement offices must be convinced that requirements are completely understood and recorded, and the manufacturers must be able to use the requirements to produce a structure around which an implementation can be developed and tested. Overcoming technical and organisational barriers and identifying requirements is not enough. Those requirements must be fit for purpose: they must meet all stakeholders needs, and they must be genuinely useful for improving and validating the systems in question.

The requirements documents are very valuable components of any election system. It would be irresponsible not to correctly manage their evolution and maintenance. But who of the current parties can we trust to do this in a competent manner?

References

Cetinkaya, O. and Cetinkaya, D. (2007) ‘’Verification and Validation Issues in Electronic Voting’’,*The Electronic Journal of e-Government*, Vol 5, No. 2, pp 117-126.

Commission for Electronic Voting (CEV) (2006) *Second report of The Independent Commission on Electronic Voting and Counting at Elections, established by the Government of Ireland* [online] http://www.cev.ie/htm/report/download_second.htm

Council of Europe (CoE) (2003). “Specific terms of reference (IP1-S-EE) of the multidisciplinary ad hoc group of specialists on legal, operational and technical standards for e-enabled voting”.

Council of Europe (CoE) (2004). “Recommendation on legal, operational and technical standards for e-voting”.

Everett, S.P. (2007) *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*, PhD Thesis, Rice University, Houston, TX, USA.

Election Science Institute (ESI) (2006) *DRE Analysis for May 2006 Primary Cuyahoga County, Ohio* [online] http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf

Federal Election Commission (FEC) (2002). "Voting systems standards". [online] http://www.fec.gov/agenda/agendas2001/mtgdoc01-62/mtgdoc01-62.html

Gibson J.P. (1997) "Feature Requirements Models: Understanding Interactions", *Feature Interactions In Telecommunication Networks IV*, IOS Press, pp 46 – 60.

Gibson J.P. (2007) "E-Voting and the Need for Rigorous Software Engineering - The Past, Present and Future, *Proceedings of the 7th International B Conference,* Springer Verlag Lecture Notes in Computer Science LNCS Vol *4355*, p1.

Gritzalis D. (2003) "Secure Electronic Voting", *Advances in Information Security*, Vol 7. Springer

Groth J. (2004) "Evaluating security of voting schemes in the universal composability framework". In *Applied Cryptography and Network Security*, Springer, Lecture Notes in Computer Science, Vol 3089, pp 46-60

Gunter, C. A., Gunter, E. L., Jackson, M., and Zave, P. (2000) "A Reference Model for Requirements and Specifications". *IEEE Software* Vol 17 No. 3 pp 37-43.

Herrnson P.S., Bederson B.B., Lee B., Francia P.L., Sherman R.M., Conrad F.G., Traugott M, Niemi, R.G. (2005), "Early appraisals of electronic voting". *Social Science Computer Review* Vol 23 No. 3, pp 274-292.

Horst, M., Kuttschreuter M. and Gutteling J. M., (2007) "Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands". *Computer Human Behaviour*, Vol 23 No. 4, pp 1838–1852.

Kocher P. and Schneier B. (2004) "Insider risks in elections". *Communications of the ACM*, Vol 47 No. 7, p104

IEEE (1993) *IEEE Std. 1219: Standard for Software Maintenance*, IEEE Computer Society Press.

Jones, C. (1996) Strategies for managing requirements creep. *Computer,* Vol 29, No. 6, pp 92-94.

McGaley, M. and Gibson, J.P. (2003) "E-Voting: A Safety Critical System". Technical Report NUIM-CS-TR-2003-02, National University of Ireland, Maynooth, Computer Science Department. [online] http://www.cs.nuim.ie/research/reports/2003/index.html#02

McGaley, M. and McCarthy, J. (2004) "Transparency and e-Voting: Democratic vs. Commercial Interests". *Electronic Voting in Europe*, pp 153-163.

McGaley M. and Gibson J.P. (2006) "A critical analysis of the council of Europe recommendations on e-voting", *EVT'06: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop.*

Mercuri R.T. and Camp L.J. (2004) "The code of elections*". Communications of the ACM*, Vol 47 No. 10, pp 52-57.

New York Times (NYT) (2007), "California Sues a Voting Machine Maker Over Changes", November 21, [online] http://www.nytimes.com/2007/11/21/us/21vote.html

Neumann P.G. (1990) "Inside risks: risks in computerized elections". *Communications of the ACM,* Vol 33 No.11, p 170.

Venice Commission, European Commission for Democracy Through Law (2002). "Code of good practice in electoral matters".

Volkamer M. and McGaley M. (2007), "Requirements and Evaluation Procedures for eVoting," *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pp. 895-902.