

Just Like Paper and the 3-colour protocol: a voting interface requirements engineering case study

J Paul Gibson
Le département Logiciels-Réseaux (LOR)
Telecom Sud Paris, TSP
9 rue Charles Fourier, 91011 Évry cedex, France
Email: paul.gibson@it-sudpais.eu

Damien MacNamara and Ken Oakley
Department of Information Technology,
Limerick Institute of Technology,
Moylish Park, Limerick, Ireland.
Email :Damian.McNamara@lit.ie and Ken.Oakley@lit.ie

Abstract—We report on the development of a novel electronic vote machine interface, with emphasis on the requirements engineering process. In particular, we review how we followed an operational prototyping approach in order to gain a better understanding of requirements in an incremental fashion. Our most interesting observations are concerned with the evolution of our most fundamental requirement: that the voting process followed by the voter should be *just like paper*. We comment on how the weakening of this requirement was deemed necessary by the addition of other requirements that were identified during our prototype evaluation. This weakening was minimized through the specification of a passive voting protocol that provides feedback to voters without obliging them to follow a voting process any different from that which is normally done using a traditional paper vote. The protocol is based on a simple 3-state machine where we naturally represent the states using the familiar traffic light colour scheme: thus the interaction between voter and interface became known as the *three colour protocol*.

Keywords—prototyping, requirements, evolution, validation

I. INTRODUCTION: VOTING SYSTEM INTERFACE REQUIREMENTS

It has been long known that requirements engineering is a key stage in the development of software systems[1]. Initially, we had a vague understanding of the innovation that our system was to offer — the electronic system was to be *just like paper* from the point of view of the voter — but the interaction between the innovative features and the foundational requirements was not so clear (which is a common issue in e-voting systems[2]). Thus, we chose to follow a development process based on prototyping, where our requirements and prototypes would be developed incrementally and in parallel. Emphasis was placed on validating each prototype against requirements, and evolving requirements based on user feedback during validation. The validation process was based on using each prototype in a real-world election. For each prototype implementation we documented the different ways in which the requirements were to be met. The traceability of requirements was critical to the success of our development process.

We note that our main contribution is a generic interface

(front-end) to a range of possible voting system back-ends. The system — known as DualVote (see section II) — uses a hybrid pen to record an electronic and paper vote simultaneously. Vote counting is beyond the scope of our system, though it is implemented during validation testing.

In our research and development, we chose to focus on usability issues. However, we are aware that such a front-end must strive to not weaken other fundamental voting system criteria which the back-end systems work hard to meet:

- **Accuracy** — it is clear that any voting system should be accurate in the sense that it returns the correct result. This can be divided into two aspects: each voter’s intended vote must be correctly recorded and each vote that is recorded must be correctly counted. This requirement is implicit in the development of any voting system; and the only differences between system requirements are with respect to the degree of error that is acceptable. As our system is a voting machine interface, our main accuracy requirement is concerned with accurate recording of the voter’s intent. Our goal is to have a system that does no worse than a paper system, and where there is a guarantee of coherency between the paper and electronic records.
- **Verifiability** — through the generation of a paper trail, our interface would, arguably, strengthen the verifiability of any voting system back-end to which it was connected.
- **Coercion-freeness** — the interface is designed to be used in isolation. It does not introduce any additional link between voter and their vote, and there is no receipt produced. It may be able to tell how the voter is voting, but it does not know the identity of the voter.
- **Security** — clearly our interface is open to attack. The paper trail significantly increases the chances of detecting successful attacks on the interface components, but does not make our interface any more secure. The new technology in our interface — a hybrid pen and RFID tags — should not introduce any additional security risks over and above those normally seen in any other

voting interface. We return to this question when we consider potential weaknesses of our system.

Our interface front-end is intended to be generic, so we have the additional requirement that the system configuration process (joining our front-end to any existing back-end) be as simple as possible. We aim to meet this requirement through the specification of a simple interface protocol between them. This protocol requires the back-end to be able to analyse the marks made by the voter on the paper (in real time) and to provide feedback on the validity of the vote (see section VI).

The remainder of the paper is structured as follows. Section II gives a brief introduction to the DualVote system, and section III describes related work. Section IV reviews the operational prototyping process that was the basis of our approach to requirements engineering. Section V reports on the three increments that our prototype went through before we were happy that we had a complete and coherent understanding of the system requirements. Section VI provides details on our final requirements specification, with emphasis on a minimal weakening of the *just like paper* requirement through the modelling of the *3-colour feedback* protocol. In particular, this section examines how the duality of each vote (in paper and electronic form) introduces coherency requirements that interact with the proposed protocol in an interesting way. We conclude the paper in section VII, where we review the strengths and weaknesses of our system.

II. THE DUALVOTE SYSTEM: BACKGROUND AND MOTIVATION

Poorly designed voting interfaces increase the effort required to vote and at worst they may interfere with the voters ability to vote as intended[3], [4]. Further, voters prefer a short and quick voting experience with a clear inverse relationship between effort and satisfaction. Our research supports the view that paper ballots require the least amount of actions from the voter in order to record their vote when compared to other types of voting system interfaces[5], [6]. We were further motivated by e-voting interface studies — such as seen with Prêt-à-Voter[7] and Punchscan[8] — that demonstrated the importance of not deviating from voters’ mental models when designing interfaces.

There have been widespread concerns with the introduction of electronic voting technology[9], [10], [11], and much criticism of systems were voters have to blindly trust the correct operation of the system and the results produced[12].

Increasing emphasis is now being placed on the ability to formally verify[13] the results of an electronic voting system. Particular importance is placed on the ability of individual voters to verify that their vote was counted and that it was counted correctly.

A simple solution would be for every voter to mark their ballot with a unique identifier, and for them to check that their vote was correctly counted. However, such a solution

is not consistent with the usual requirement for coercion-free[14] elections or anonymous voting. The verifiability of paper elections is usually guaranteed through an observable election process, where any voter is free to remain in the voting office and physically follow the ballots as they are recorded and counted. Anonymity can be guaranteed by ensuring that there are no distinctive markings on ballots that can tie a ballot to a particular voter. Verifiability takes the form of an observer being able to witness that every ballot that is deposited in the urn is correctly counted (without knowing who voted for whom).

The DualVote system addresses the crucial issues of usability and verifiability by providing an electronic voting machine interface where votes are recorded by electors using a paper and pen. The recording of the vote generates simultaneously a paper hard-copy of the vote as well as an electronic copy. Thus, without placing any additional constraints or procedural requirements on the voter, the votes can be counted both manually and electronically.

We have already reported on the technologies used in implementing such an interface, and usability studies from experiments where DualVote prototypes have been deployed for real elections[15], [16]. In this paper we focus on the role that the prototypes have played in our understanding and modelling of the system requirements.

III. RELATED WORK

Usability issues for traditional e-voting systems have been addressed in [4]. Usability issues introduced by electronic interfaces are addressed in a number of different papers, for example:[5], [6]. The issue of poor interface design is reported by Roth[17]. Problems with providing feedback through a review screen are discussed in Everett’s thesis[18].

Alternative approaches to providing a hybrid user interface are presented in the Punchscan system[8], which uses optical scanner technology, and a *Better Ballot Box*[9], which integrates a printer mechanism in the system in order to provide a paper trail. In optical scan systems where pen and paper may be used to vote, there are two general tasks that need to be carried out in order to vote. Firstly, the voter must vote by usually punching a hole or shading in an area on the paper ballot. Secondly the ballot paper has to be fed into a scanning apparatus. DualVote permits total freedom in what the user writes with the pen, but increases the risk of the recording of a spoiled (invalid) vote. Further, DualVote does not require an additional scanning process — the scan is done without the voter being aware of the process. A study by Goggin et al.[19], which examined the practicalities of using a VVPAT system attached to a voting machine, revealed significant delays in processing the paper receipts as each receipt had to be separated from a spool of paper before counting. This illustrates the type of problem that can occur when a printer is a component of an e-voting

system. No printer is required in DualVote, so these issues are not relevant.

Using formal modelling and verification to ensure that an interface cannot generate invalid votes is reported in *Refinement: A Constructive Approach to Formal Software Design for a Secure e-voting Interface*[20].

Recently, Oren and Wool have reviewed potential problems with using RFID technology in voting systems[21].

IV. PROTOTYPING FOR REQUIREMENTS ENGINEERING

In the uptake of any system, the support of future users is often a critical factor. A system that is developed without input from the targetted users has two main problems. Firstly, it is unlikely to do what the users would like it to do. Secondly, it is unlikely that the users will be enthusiastic about its deployment. Users are often very good at criticising a concrete system, whilst being unable to comment on abstract models. In particular, a concrete system helps users to better understand and express their needs. As a secondary benefit, a prototype can improve communication between the users and the developers. This is vital where the problem domain and solution domain are separated by different languages and concepts. In effect, a prototype acts like a common framework for discussion between the two different groups. Finally, encouraging user feedback increases the likelihood that future users will be enthusiastic about adopting the new system/technology.

Given that we had a poor understanding of our requirements, and that we wanted to build an enthusiastic user base, we considered prototyping to be an ideal development process. We did not make a conscious decision to follow a specific prototyping process, but through retrospective analysis it was clear that we were following a process which was a mix of rapid (throwaway) prototyping and evolutionary prototyping. Further investigation led us to discover that our approach could be best classified as operational prototyping[22].

A. Rapid Prototyping

A clear objective in the DualVote project was to increase the frequency with which we could experiment with our system through the running of real elections. Our intention was that the prototype would not be the final version of the system, but that the final version would be built from scratch. This *throw-away* approach is a characterisation of rapid prototyping. However, our approach differed from rapid prototyping because we evolved a sequence of prototypes as our understanding evolved.

B. Evolutionary Prototyping

Evolutionary prototyping has a main goal of building a robust system as quickly as possible. The parts of the system that are well understood are built rigorously and parts that are not well understood are not necessarily incorporated

into the current increment of the prototype — leading to incompleteness. As the prototype evolves, the system becomes better through becoming more complete.

We required our prototype systems to be used in real elections — as part of the validation process — and so required that our prototypes be complete. Thus, although we were evolving our system we were not following the evolutionary prototyping process.

C. Operational Prototyping: finding a compromise

Operational prototyping offers many advantages when trying to build a better understanding of the requirements of a system[22]. It is a specialisation of software prototyping which focuses on finding a good balance between stability and rapid results. We became aware that we were following such an approach only after we had carried out 3 increments in our development, and were trying to get a better understanding of the process that we had followed.

D. Prototyping for building understanding: the analysis process

It is beyond the scope of this paper to provide details of the testing and usability studies, which focused on voter satisfaction, efficiency and accuracy: the interested reader can find such information in other published papers[15], [16], [23]. However, the overall process is quite general and merits further discussion.

The system usability scale (SUS), proposed by Brook[24], formed the basis of our objective set of usability criteria. (This also permitted comparison with other systems evaluated against the same scale.) During every development iteration, we evaluated our prototypes on this scale, identified weaknesses where the scores could be improved and made design changes in order to address the perceived weaknesses.

Further, a subset of voters provided unstructured feedback (written and spoken) concerning general requirements of voting systems and whether our system met their expectations. Such feedback helped us to identify requirements that had been overlooked or misunderstood. In some such cases, the requirements had to be updated and decisions made as to whether the system design could support such changes, or whether a design change had to be made.

The most interesting analysis arose out of inconsistent feedback — where different users (and different types of users) had contradictory requirements or contradictory opinions of the system under test. The SUS tends to average out such disagreements and this valuable information can only be fully leveraged through subjective analysis by domain experts. This is currently the weakest part of our development process. We have no procedures for dealing with such requirements interactions, and deal with them in an ad-hoc manner. However, such interactions are explicitly documented.

V. REQUIREMENTS EVOLUTION

In the following subsections, we examine the first three prototypes that were developed, based on three different technologies: a camera, an inductive sensor array and an optical sensor array. For each of the three prototypes we comment on:

- The requirements and, if appropriate, how they have changed from the previous prototype iteration.
- Implementation decisions that were made.
- Validation and requirements analysis, where feedback from our experiments (elections) fed forward into the development of the next prototype.

Through the evolution of our system we used a simple naming scheme to keep track of changes to requirements: when a requirement is updated we add the index corresponding to the current prototype iteration; and when a requirement is added we label it with a new indice. This naming scheme should assist the reader in the remainder of this paper, where we detail the steps that we followed in arriving at a stable set of complete and coherent requirements.

A. Prototype 1: Camera Based Technology

The first prototype was developed in order to get a better understanding of the requirements of the system, and the capabilities/limits of the technology selected for implementation. The original requirements documentation for this prototype was a number of pages long and was poorly structured. In this paper, we present a summary of the main requirements that were evident in this first requirements document through a retrospective analysis that was carried out after the development of the third prototype.

- **Req1-1_P&P:** The voter completes their ballot using pen and paper (P&P). They must have no perception of using an electronic device, and should place their completed paper ballot in a physical urn in the “traditional way”. This requirement will guarantee the generation of a “pure paper trail” — i.e. one in which all completed ballots are recorded on a non-electronic medium and the generation of this record is not dependent on any electronic technology.
- **Req2-1_Duality:** The process of voting shall produce an electronic copy of the completed ballot which is guaranteed to be coherent with the paper ballot, without placing any additional requirements or constraints on the voter compared with the “traditional voting process”. For each physical ballot that is placed in a physical urn there will be an equivalent electronic ballot stored in an electronic urn.
- **Req3-1_Passivity:** There will be no need for users of the system to activate any of the electronic components of the system during the stage of the election process when the voting booths/urns are open for voting.

- **Req4-1_QoS:** The time to complete a ballot and place it in the urn will be no longer than for the “traditional method”.

Note, at this stage, that security was not a foundational requirement but an aspect of the system which cross-cuts most (if not all) other requirements. We return to the question of security in the conclusions section.

The first prototype of the DualVote system adopted a simple optical interface using a camera placed underneath a transparent writing surface. The camera detected printed markings on the underside of the ballot paper in order to determine the paper orientation. The voter made their selections using a certain type of ink marker and the camera read a mirror image of the ink marks through the underside of the ballot paper which was of a particularly light grade. Through this process the system could identify how the vote was cast.

Additionally the DualVote concept included the novel use of Radio Frequency Identification (RFID) technology to facilitate the activation of the voting machine and to maintain consistency between the electronic and paper votes. The authors devised the idea of “transparent activation” which meant that neither the voter nor the poll worker should have to perform any extra action to cause the voting machine to activate. To this end, a RFID tag was added to the ballot paper. When the voter placed the ballot paper on the writing surface, the RFID tag communicated with an RFID reader located near the writing surface, but out of the view of the camera, thus activating the machine automatically. The RFID tag also ensured that the ballot paper could not be removed from the polling station. If the RFID tag associated with a particular ballot paper was not detected in the ballot box, then the electronic vote would not be counted, thus maintaining consistency between the electronic and paper ballots.

Through feedback from the first validation of the prototype, we became aware of 4 main issues:

- Folding the paper ballot compromised the correct recording of the electronic vote. This means that the system fails to adequately meet requirement **Req2-1_Duality**.
- The voting process required voters to confirm (electronically) their candidate selections on the completed ballot. Thus, prototype 1 does not adequately meet requirement **Req3-1_Passivity**.
- Voters were concerned that the camera technology could be exploited to take a photograph of them whilst voting and therefore compromise their anonymity. As our initial requirements make no mention of anonymity, our initial requirements list was deemed to be incomplete.
- Using RFID technology has many security issues[21] that concern some voters. As our initial requirements

make no mention of security, our initial requirements list was deemed to be incomplete.

There were no issues with requirements **Req1-1_P&P** and **Req4-1_QoS**. In particular, the first prototype tests demonstrated that voters were able to vote at the same speed as they would have voted with the traditional pen and paper. (This was not a surprise, but it was important to validate that our intuition that a *just like paper* system would share common properties with the paper system on which it was based.)

B. Prototype 2: Using Inductive Technology

We started by restructuring the **Duality** and **Passivity** requirements. There was a fuzzy interdependency between these requirements that needed clarification. Namely, the **Duality** subphrase “without placing any additional requirements or constraints on the voter compared with the “traditional voting process”.” would seem to guarantee **Passivity**. Thus we chose to move this subphrase from **Duality** to **Passivity**. We then added a requirement for anonymity. Finally, we re-worded the pen requirement to be less demanding in order to facilitate a change to our pen technology.

Thus, the new requirements were documented as follows:

- **Req1-1.2_P&P:** The voter completes their ballot using pen and paper (P&P), and should place their completed paper ballot in a physical urn in the “traditional way”. This requirement will guarantee the generation of a “pure paper trail” — i.e. one in which all completed ballots are recorded on a non-electronic medium and the generation of this record is not dependent on any electronic technology.

Change 1 to 2 — removed the requirement that there should be no perception of using an electronic device. This change will facilitate the use of an electronic pen, provided its functionality is perceived to be equivalent to a “traditional” pen.

- **Req2-1.2_Duality:** The process of voting shall produce an electronic copy of the completed ballot which is guaranteed to be coherent with the paper ballot. For each physical ballot that is placed in a physical urn there will be an equivalent electronic ballot stored in an electronic urn.

Change 1 to 2 — removed the subphrase “without placing any additional requirements or constraints on the voter compared with the “traditional voting process”.”.

- **Req3-1.2_Passivity:** The voting process will not introduce any additional requirements or constraints on the voter compared with the “traditional voting process”. This includes the requirement that there will be no need for voters to activate any of the electronic components of the system. We also require that such activation be automated so that there is no need for election officials to fulfil this task.

Change 1 to 2 — added the subphrase “without placing

any additional requirements or constraints on the voter compared with the “traditional voting process”.” and explicitly separated passivity of election officials from that of voters..

- **Req4-1_QoS:** *Unchanged*
- **Req5-2_Anonymity:** Anonymity must be enforced and be seen (by the voter) to be enforced.

The second prototype was entirely removed from optical technologies. The reason for this move was due to the perception that any optical embodiment of the DualVote system would be seen to compromise voter anonymity.

This second prototype contained a novel Inductive Sensor Array Reader (ISAR). The implemented ISAR was comprised of an array of 42x32 inductors and is the size of a typical voter writing surface (378mm x 288mm). The ISAR worked on the principle that metallic materials of a certain magnetic property will cause a change in the inductance of an inductor in the array when brought close to that inductor. The ballot paper in the Dual Vote system had metallic marker strips attached to the underside. When placed on the writing surface, these metallic marker strips caused the change in the inductance of certain inductors in the array. This inductance change was captured by a measurement system and passed to the system software effectively as a bitmap image. Standard machine vision algorithms were then used to calculate the ballot paper location in relation to the known position of the metallic strips. Unlike the camera solution, the ISAR may not be used to record the voter’s intentions using a non-electronic ink pen. This led to the separation of the UI design process into distinct divisions:

- (i) Identification of the orientation of the paper form on the writing surface (Locator)
- (ii) Determining the voter’s intentions (Interpreter).

Commonalities were initially identified between the first and second prototypes with regard to ballot paper design in that markers needed to be placed on the back of the ballot paper to help determine the voter’s intention. With regard to the ISAR prototype however, these markers served only to allow the software to determine the orientation of the ballot paper and did not give an indication as to the position of the preference boxes. Furthermore the composition of these markers was non ink-based and could not be traditionally printed using standard printing technologies.

The ink pen which was initially non-electronic in the first prototype became a hybrid electronic and ink pen. This was due to the separation of the interface into the locator and interpreter components. This hybrid-pen was connected to a transparent digitizer and placed on top of the ISAR. A transparent digitizer was chosen so that the original camera-based approach in the first prototype could technically be facilitated in the event of a problem with the inductive sensor array; however this never arose. Note that the second prototype no longer required voters to validate their ballot.

The introduction of an electronic pen did not raise any issues as feedback from voters validated **Req1-1.2_P&P**, but we continued to have problems in validating **Req2-1.2_Duality**. Removing the need for voter validation of ballots addressed one of the issues with respect to **Req3-1.2_Passivity**. However, there was a technical limitation of the ISAR hardware that compromised the use of the RFIDs: the interference produced by the RFID antenna (which needed to be large enough to detect a ballot paper placed anywhere on the writing surface) prevented the correct operation of the hardware. As a consequence, the election administrators were required to activate the machine between voters. Thus, the requirement of voter passivity was met but not the requirement for passivity in general.

At this point in development, feedback from the voters led us to question whether the passivity requirement would compromise the users' trust in the correct functioning of the system. For the initial prototype, where the voters had to actively validate the electronic ballot record, this appeared to provide a degree of reassurance. In the second prototype, where no such validation was required, we certainly provided an interface that was closer to the "traditional" voting experience but the voters — being aware that there was an electronic record being produced — were uncomfortable with having to trust the machine to guarantee that their e-ballot was correctly recorded. (Of course, the paper trail should reassure them that the election process is verifiable, but this is not obvious to most voters.)

A final issue arose from minor problems with the electronic pen — it was not 100% reliable and for a small number of votes (around 2%) there was inconsistency between the electronic and paper ballots.

C. Prototype 3: Optic Sensor Array Technology

In the iterative prototyping approach, we expect that requirements stabilize as we gain a better understanding of the system at different levels of abstraction. This is evident in the third prototype where most of the previous requirements were unchanged; and we only added requirements in order to address dependability problems witnessed in the first two prototypes:

- **Req1-1.2_P&P:** *Unchanged*
- **Req2-1.2_Duality:** *Unchanged*
- **Req3-1.2_Passivity:** *Unchanged*
- **Req4-1_QoS:** *Unchanged*
- **Req5-2_Anonymity:** *Unchanged*
- **Req6-3_Dependable:** The system and its components must be dependable[25].
- **Req7-3_Feedback:** If a component failure compromises the recording of an e-ballot, then the voter will be informed so that they may retry to record their ballot (perhaps at a different machine).

With regards to the second prototype, difficulties arose with non-flat (folded or crumpled) ballot papers. If the ballot

paper was raised in any way prior to being placed on the voting surface, the metallic markers may be outside the detection distance of the ISAR. If enough sensors did not activate then the position of the ballot paper could not be determined by the software and hence the electronic vote not cast.

In addition, the fabrication of ballot paper with affixed metallic strips added a financial overhead to the ballot paper we considered replacing the inductors with optical sensors which were not capable of capturing an image of the voter. This would allow the replacement of the metallic strips with printed ink markers.

In order to overcome the privacy limitation discovered while building the first prototype, the authors explored an alternative optical technology. This implementation — in the third prototype — consisted of an array of light emitting diodes (LEDs) and infra-red sensors. This interface is termed OSAR (Optical Sensor Array Reader).

In this interface, the back of the ballot paper is marked again with ink markers which lower the reflectivity if lit with IR light. The ink used is standard laser printer toner. The amount of reflected light is detected by the IR detectors. Both LEDs and detectors are lensed and positioned in such a way as to optimise the spatial resolution of the system.

The metallic strips on the ballot paper are replaced with ink markers (patterns) which are simply printed directly onto the ballot paper. The authors used an 8x8 array of rectangles; for this array there are 2^{64} possible patterns representing the binary possibilities of 1 for white and zero for black. Equal numbers of black and white rectangles were chosen. The pattern was also designed to avoid large areas of solid black or white space. This minimizes the likelihood of false positive correlation with other accidental patterns in the image.

Validation of the third prototype identified only two outstanding issues with respect to meeting the current requirements:

- **Req3-1.2_Passivity** — Transparent activation is not supported due to outstanding hardware limitations of the RFID tags.
- **Req5-2_Anonymity** — We identified a potential breach of the fundamental anonymity requirement which may be unique to pen based e-voting systems. A warning system was implemented to notify the poll worker if no pen coordinates are being received by the software (to catch any potential faults with the hybrid pen) and to meet requirement **Req7-3_Feedback:**. However if the voter intended to spoil their vote by casting a blank ballot, then this warning notification could in fact reveal the voter's intention.

After the third iteration we were confident that our overall design (and choice of hardware technology) was able to meet our requirements. The RFID interference problems should be easy to solve using current technologies. The single

outstanding issue was that of providing feedback to the voter without compromising the *just like paper* objective. These problems are considered in more detail in the next section.

VI. Just Like Paper AND THE 3-Colour Protocol

At this stage of development we were sure that we had a very good understanding of our requirements and that these individually would be unlikely to be changed in future versions of the system, even if we added new requirements. We were also confident that the optical sensor array technology was our best alternative. As the system design was also stable, we hoped that the fourth prototype would be a final demonstrator that could be used when working with future clients. Thus, in order to increase the number of possible clients, we chose to add a requirement that would make our e-voting system as generic as possible: see **Req8-4_Generic**. Finally, being aware of the issues regarding proprietary e-voting system components[26], we add a requirement — **Req9-4_NonProprietary** — that all system components be non-proprietary. These two requirements were considered to be orthogonal to already existing requirements.

A. Final requirements specification

- **Req1-1.2_P&P:** *Unchanged*
- **Req2-1.2_Duality:** *Unchanged*
- **Req3-1.2_Passivity:** *Unchanged*
- **Req4-1_QoS:** *Unchanged*
- **Req5-2_Anonymity:** *Unchanged*
- **Req6-3_Dependable:** *Unchanged*
- **Req7-3_Feedback:** *Unchanged*
- **Req8-4_Generic:** The interface will be able to record any type of vote provided the list of options is known (fixed) in advance¹
- **Req9-4_NonProprietary:** All system components will be nonproprietary.

The major outstanding issues in meeting these requirements are:

- **Req3-1.2_Passivity:** — how to achieve passive activation of the machine using RFID technology
- **Req6-3_Dependable:** — how to achieve acceptable levels of dependability in the electronic pen and sensors
- **Req7-3_Feedback:** — how to provide feedback without compromising **Req5-2_Anonymity** or **Req3-1.2_Passivity**.

In the remainder of this paper we focus on meeting the feedback requirement — the others are technology issues which should be easily achievable. In contrast, it is not clear how to best integrate **Req7-3_Feedback** with **Req5-2_Anonymity**, **Req2-1.2** and **Req3-1.2_Passivity**. In the following we propose a simple protocol as a possible solution.

¹We are currently investigating whether the technology can also be used for elections with write-in candidates.

B. The 3-colour protocol

In order to respect the passivity requirement (**Req3-1.2_Passivity**) we decided that our feedback procedure should be informative and require no additional actions from the voter in order to record a vote. The choice of what feedback to provide would be critical when we consider how this requirement interacts with the others.

The richest form of feedback would be for the machine interface to present to each voter an interpretation of the voter’s completed ballot. This would reassure voters that the machine was able to correctly interpret their vote; but more sceptical voters would realise that this did not necessarily mean that this was the vote that was actually recorded. Such rich feedback introduces an extra risk: a voter who wished to undermine confidence in the machine could claim that their vote was incorrectly interpreted. It would be very difficult to address this risk without introducing a more complicated voting process which involves some trusted third party checking such a claim.

In order to avoid such complexities, we decided that the feedback should not say how the machine had interpreted the ballot, but should state only whether the ballot could be interpreted. On first sight, it would appear that we need only boolean feedback — to separate spoiled from unspoiled votes. However, in its initial state, a ballot has no marks on it; and this is normally considered to be a blank vote. Thus, we introduce an initial third state for when a ballot is undecided: from this state the voter can choose to record a spoiled or unspoiled vote. Note that a voter can always make a spoiled vote from an unspoiled vote; but can never reverse the spoiled option². Note also that a voter can choose to put a ballot in any of the three states into the urn.

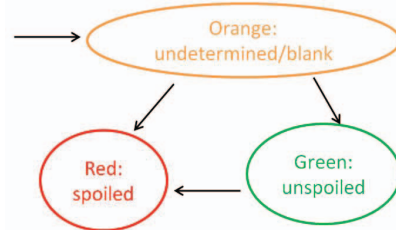


Figure 1. 3-colour Protocol: finite state machine

This protocol meets our generic requirement (**Req8-4_Generic**) as an undetermined state also applies to other interfaces where the election rules state that a valid vote consists of making more than one selection.

We plan to implement the transition out of the initial undetermined state by some threshold value corresponding to the amount of ink/writing on the ballot paper. This is particularly important if we wish to guarantee our anonymity

²This property may be unique to pen-based systems.

requirement (**Req5-2 Anonymity**), which is compromised if voters can leave identifying marks on the ballot paper. Anonymity is also respected for spoiled (and blank) votes: only the voter is aware of the feedback state and so election officials cannot tell what type of vote is recorded.

The feedback requirement was introduced to reassure voters that the machine has been able (or not) to interpret their voting intention. We need to specify the procedure to be followed if a voter is unable to record an unspoiled vote. Quite simply, if a voter sees a red state and they wish to record an unspoiled vote then they must get a new ballot paper. In the unlikely situation that they are unable to spoil their vote, they are advised to try a new machine (and a new ballot). When a machine is faulty, election officials should observe many voters requesting new ballots — and they will be able to take appropriate action without compromising anonymity.

We note that the feedback is passive. Voters are not required to take notice of the ballot state — it is an optional reassurance that requires no additional action from the voter. However, we do acknowledge that it slightly weakens our claim that DualVote is *just like paper*.

C. The coherency problem

The use of a paper ballot ensures that there is a voter verifiable audit trail. Thus, we can always verify the electronic result against a paper (re)count. Random sampling may be used to reduce the number of paper counts required during the verification of an election. Independent of the number of samples, a problem arises if the two counts are not coherent with each other. When this happens, the paper count must be given priority over the electronic count. If the paper count is compromised in any way then it is probably not a good idea to default to the results of the electronic system (unless sampling has established a very high coherency in areas where the paper count has not been compromised).

The risk of incoherent counts is therefore one of confidence and resources. Such incoherence will quickly lead to confidence in the electronic system being eroded. Furthermore, the more times that incoherent counts occur, the more resources are needed to perform the paper counts. Thus, it is in the best interest of all parties that the electronic and paper counts return the same result (within well-defined bounds).

The main issue is not in incoherency between the counting processes: building a correct software count is reasonably straightforward[27]. Where inconsistency is most likely to arise is in the interpretation of ballots which have been completed by pen. In particular, we focus on the issue of spoiled votes. Two situations that should be minimized by any election process are:

- The voter intends to spoil their vote, yet their vote is wrongly allocated to a candidate.
- The voter does not intend to spoil their vote, yet their vote is wrongly interpreted as being spoiled.

The feedback from the *3-colour protocol* should address inconsistency problems arising from an unreliable interface. However, inconsistency in counts will always occur if the human interpretation of whether a vote is spoiled is different from that of the machine. The feedback to the voter means that we can ignore cases 3,4,5 and 6. Cases 1 and 8 are not problematic. Thus, there are 2 problematic cases — 2 and 7.

Voter Intent	Electronic Count Machine Interpretation	Paper Recount Human Interpretation
1 Unspoiled	Unspoiled	Unspoiled
2 Unspoiled	Unspoiled	Spoiled
3 Unspoiled	Spoiled	Unspoiled
4 Unspoiled	Spoiled	Spoiled
5 Spoiled	Unspoiled	Unspoiled
6 Spoiled	Unspoiled	Spoiled
7 Spoiled	Spoiled	Unspoiled
8 Spoiled	Spoiled	Spoiled

Figure 2. Coherency matrix

We propose that all spoiled votes (as interpreted by the machine) should be verified by a human (in a partial recount)³ This handles case 7, leaving only case 2: when the machine interprets a vote as being unspoiled whilst the paper count considers it to be spoiled. Our analysis suggests that this case is the most unlikely to occur. DualVote passes responsibility for this potential problem to the clients of the interface — they must provide the component that determines whether or not a vote is spoiled. We discuss this further in the conclusions section where we introduce a final requirement — **Req10-4 Pluggable** — for connecting the interface *front-end* to any voting machine *back-end*.

D. Pluggability

During our experimentation (with real elections) we were required to build the voting machine *back-end*: to validate the interface we have to count the votes both electronically and by hand. To this end, we have to be able to interpret the electronic ballots. This interpretation can be done at the *front-end* or the *back-end*. In order to meet our generic requirement (**Req8-4 Generic**) this must not be done in the interface. Thus, the final DualVote prototype provides a formally specified interface to permit the *back-end* of any voting machine to process a recorded ballot (in real-time) and provide the necessary *3-colour protocol* feedback to the voter. For completeness, we add the final requirement:

- **Req10-4 Pluggable:** The interface will provide a formally specified real-time interface to drive the *3-colour protocol*.

We are currently testing the pluggability of our interface by connecting to a back-end which implements the Prêt à voter[7] voting protocol.

³If this becomes a significant number of votes then this certainly warrants detailed analysis, and the additional cost should be acceptable.

VII. CONCLUSIONS

DualVote is a generic e-voting interface. Our requirements focus on the interface — the *front-end* — rather than the whole voting machine; yet they take into account common issues such as usability, accuracy, verifiability, coercion-freeness, security, etc . . .

As with all systems involving complex, interacting requirements, design is a process of finding a good compromise; leading to each system exhibiting its own strengths and weaknesses. In the following we review our own understanding of these with respect to the DualVote user interface.

A. Strengths

The main strength of our system is in usability. All our trials have shown high usability scores when compared with other voting systems.

An advantage of our hybrid system over the traditional paper system, which it is designed to improve upon, is that the voter gets immediate feedback that their vote is marked as intended. The degree of feedback is currently limited to informing the voter as to whether their vote is considered, by the electronic system, to be valid, spoiled or blank. This feedback was specifically introduced to address the problem of incoherency between the paper and electronic counts with respect to identification of spoiled votes. Current trials are intended to show that this feedback may assist the voter in having their intent correctly recorded. This should demonstrate that the system is more accurate than a purely paper system.

The duality of our approach allows for mutual verifiability: the paper trail can be used to audit the electronic system and/or the electronic system can be used to audit the paper system. Our interface does not preclude some sort of end-to-end verification scheme. These would be complementary: our mutual verifiability is much easier to understand than current schemes involving complex cryptographic techniques, and the end-to-end verification can probably demonstrate election accuracy (if one is willing to trust the cryptographic processes).

B. Weaknesses

We have not yet considered the security of our system with respect to malicious attacks. As the interface developers, we have implicit trust in the security of the development process. Currently, we assume that the polling staff are honest, and that voters will not attempt to purposely cause (or claim) inconsistencies. Our interface is neither more nor less susceptible to attacks from other external sources. The duality of the system, together with a VVAT makes it very difficult for an attacker to compromise an election without it being detected. However, an attack on either the paper ballots or the electronic ballots could lead to inconsistent counts, and this would certainly compromise the users' trust in the correct functioning of the system as a whole.

We are aware that voting machine security[28] cannot normally be added-in after a system has already been built — it must be incorporated into the system design as early as possible. In the case of e-voting, security weaknesses are usually addressed through procedural requirements[29].

The RFID technology is certainly a secure concern that requires further research before we use it in a final system. The prototypes have shown that it can aid us in meeting the passivity requirement, but if it introduces a security weakness that could compromise our other requirements then we must take this into account.

C. Future Work

We are reluctant to enrich our feedback to incorporate additional information, such as an electronic display of the machine's interpretation of each voter's intent. This feature is appealing to voters but complicates the process for election officials as a hostile voter may be tempted to claim that the electronic display is not consistent with their intent. To address this, it may be useful to have an audit process which could test this electronic feedback during the election process. As our goal is to have a system that is *just like paper*, we are not sure that adding such an audit is worth compromising the simplicity of the current interface.

In its current form, ballots can be uniquely identified (by the RFID tags) but are not linked to voters. The tags could be used to link ballots to voters, and so the voters have to trust that this is not the case. Further, the security implications of using RFID tags are not currently fully understood. Future research will examine replacing the RFID tags with an alternative technology.

The prototyping process has been a success. The next step is to consider the mass production of such a DualVote interface. In such mass production there is a natural trade-off between manufacturing cost and robustness of the system. Our prototyping suggests that we can manufacture a reasonably robust system at reasonable cost, but our positioning on the quality-cost curve is not yet clear.

A major weakness of our requirements driven process is that we still do not fully understand how e-voting requirements interact (yet they clearly do so). As a consequence, dealing with such interactions will tend to be ad-hoc. Foundational research is needed in this area, with much more analysis of the compromises and trade-offs that exist in already existing systems. This should lead to some sort of e-voting system taxonomy based on requirements models: only then will we be able to produce voting systems that are acceptable to everyone.

REFERENCES

- [1] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the Conference on The Future of Software Engineering*, ser. ICSE '00. New York, NY, USA: ACM, 2000, pp. 35–46.

- [2] J. Gibson, E. Lallet, and J.-L. Raffy, "Feature interactions in a software product line for e-voting," in *Feature Interactions in Software and Communication Systems X*, Nakamura and Reiff-Marganiec, Eds. Lisbon, Portugal: IOS Press, June 2009, pp. 91–106.
- [3] S. J. Laskowski, M. Autry, J. Cugini, W. Killam, and J. Yen, "Improving the usability and accessibility of voting systems and products," NIST, Tech. Rep. NIST Special Publication 500-256, 2004.
- [4] M. D. Byrne, K. K. Greene, and S. P. Everett, "Usability of voting systems: baseline data for paper, punch cards, and lever machines," in *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*. New York, NY, USA: ACM, 2007, pp. 171–180.
- [5] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi, "Electronic voting system usability issues," in *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*. New York, NY, USA: ACM, 2003, pp. 145–152.
- [6] F. G. Conrad, B. B. Bederson, B. Lewis, E. Peytcheva, M. W. Traugott, M. J. Hanmer, P. S. Herrnson, and R. G. Niemi, "Electronic voting eliminates hanging chads but introduces new usability challenges," *International Journal of Human-Computer Studies*, vol. 67, no. 1, pp. 111 – 124, 2009.
- [7] D. Bismark, J. Heather, R. M. A. Peel, S. Schneider, Z. Xia, and P. Y. A. Ryan, "Experiences gained from the first Prêt-à-Voter implementation," in *Proceedings of the 2009 First International Workshop on Requirements Engineering for e-Voting Systems*, ser. RE-VOTE '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 19–28.
- [8] A. Essex, J. Clark, R. Carback, and S. Popoveniuc, "Punchscan in practice: an E2E election case study," in *Proceedings of Workshop on Trustworthy Elections*, 2007.
- [9] R. Mercuri, "Government: a better ballot box?" *IEEE Spectr.*, vol. 39, no. 10, pp. 46–50, 2002.
- [10] M. McGaley and J. P. Gibson, "E-Voting: A Safety Critical System," NUI Maynooth, Computer Science Department, Tech. Rep. NUIM-CS-TR-2003-02, 2003.
- [11] P. G. Neumann, "The problems and potentials of voting systems," *Commun. ACM*, vol. 47, no. 10, 2004.
- [12] B. Randell and P. Y. A. Ryan, "Voting technologies and trust," *IEEE Security and Privacy*, vol. 4, no. 5, pp. 50–56, 2006.
- [13] O. Cetinkaya and D. Cetinkaya, "Verification and validation issues in electronic voting," *The Electronic Journal of e-Government*, vol. 5, no. 2, pp. 117–126, 2007.
- [14] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *WPES*, V. Atluri, S. D. C. di Vimercati, and R. Dingledine, Eds. ACM, 2005, pp. 61–70.
- [15] D. MacNamara, T. Scully, J. Gibson, F. Carmody, K. Oakley, and E. Quane, "Dualvote: Addressing usability and verifiability issues in electronic voting systems," in *2011 Conference for E-Democracy and Open Government (CeDEM11)*. Danube University, Krems: Edition Danube University, May 2011.
- [16] D. MacNamara, F. Carmody, T. Scully, K. Oakley, E. Quane, and J. Gibson, "Dual vote: A novel user interface for e-voting systems," in *IADIS International Conference on Interfaces and Human Computer Interaction 2010*. Freiburg, Germany, 28 - 30 July 2010: IADIS, 2010.
- [17] S. K. Roth, "Disenfranchised by design: voting systems and the election process," *Information Design Journal*, vol. 9, no. 1, pp. 1–8, 1998.
- [18] S. P. Everett, "The usability of electronic voting machines and how votes can be changed without detection," Ph.D. dissertation, Rice University, Houston, TX, USA, 2007.
- [19] S. N. Goggin and M. D. Byrne, "An examination of the auditability of voter verified paper audit trail (VVPAT) ballots," in *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2007*. Berkeley, CA, USA: USENIX Association, aug 2007.
- [20] D. Cansell, J. P. Gibson, and D. Méry, "Refinement: A constructive approach to formal software design for a secure e-voting interface," *Electr. Notes Theor. Comput. Sci.*, vol. 183, pp. 39–55, 2007.
- [21] Y. Oren and A. Wool, "RFID-based electronic voting: What could possibly go wrong?" in *2010 IEEE International Conference on RFID*, april 2010, pp. 118 –125.
- [22] A. M. Davis, "Operational prototyping: A new development approach," *IEEE Softw.*, vol. 9, pp. 70–78, September 1992.
- [23] D. MacNamara, T. Scully, F. Carmody, K. Oakley, E. Quane, and J. Gibson, "Dual vote: A non-intrusive evoting interface," *International Journal of Computer Information Systems and Industrial Management Applications(IJCISIM)*, 2011, to appear.
- [24] J. Brooke, *Usability evaluation in industry*. London: Taylor & Francis, 1991, ch. SUS: A quick and dirty usability scale, pp. 189 – 194.
- [25] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *Dependable and Secure Computing, IEEE Transactions on*, vol. 1, no. 1, pp. 11 – 33, Jan 2004.
- [26] J. Kitcat, "Source availability and e-voting: an advocate recants," *Commun. ACM*, vol. 47, no. 10, pp. 65–67, 2004.
- [27] J. R. Kiniry, D. Cochran, and P. E. Tierney, "Verification-centric realization of electronic vote counting," in *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2007 on Electronic Voting Technology Workshop*. Berkeley, CA, USA: USENIX Association, august 2007.
- [28] D. Balzarotti, G. Banks, M. Cova, V. Felmetzger, R. A. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, "Are your votes really counted?: testing the security of real-world electronic voting systems," in *ISSTA*, B. G. Ryder and A. Zeller, Eds. ACM, 2008, pp. 237–248.
- [29] A. Xenakis and A. Macintosh, "Procedural security and social acceptance in e-voting," in *HICSS*. IEEE Computer Society, 2005.