Specification of the Control Logic of an eVoting System in UML: the ProVotE experience

Roberto Tiella
ITC-irst
tiella@irst.itc.it

Adolfo Villafiorita
ITC-irst
adolfo@irst.itc.it

Silvia Tomasi
ITC-irst
silviadik@tin.it
eVoting

- The use of electronic devices to support operations during an election

- Different types of systems (from lever machines to mobile voting systems)

- Experimented and/or adopted in various countries (with different levels of acceptance)
eVoting in Italy

- Some experimentations
  - usually on a small scale
  - usually “isolated”

- Relatively strong resistance
  - by citizens (e.g. doubts related to anonymity)
  - by politicians (e.g. will my electorate be able to vote me electronically?)
  - by public administration (e.g. alteration of data, service levels)

- Biggest experimentation at last political elections to tabulate and sending results from precincts to the Ministry of Interior

  “…The results of the electronic experimentation will have legal value only if the data agrees with those on paper.”
Context: eVoting in Trentino


Art. 84, comma 1. In order to accelerate and simplify voting and tabulation procedures [...] subjected to the approval of a Commission of the Provincial Council [...], the local Government approves a project for the automation of the procedures for electing the President of the Province and for local referenda.
ProVotE aims at giving full implementation to art. 84, by providing systems for the automation of electoral operations, reducing the risk of digital divide and that of abstentionism.

Scenario:
- full automation of the voting “chain” (from expression of the vote to dissemination of the results)
- full automation of “accessory” functions (registration, paper logs, …)

Remark: remote voting illegal in Italy
Some of the expected benefits

- **Efficiency**
  - (e.g. time currently spent to clear up *material* errors)

- **Reduction of the litigation**
  - *(eliminating it is a bit far edged)* - significant indirect cost for the administration

- **Voting in autonomy** for impaired people

- **Elimination of certain "attacks"**
  - (e.g. trying and voting blank ballots; but ...)

- **Basis for enabling forms of direct democracy**
Where we are

- mid-term
- prototypes for all the systems of the voting chain and the registration chain
- development process based on UML/StateMachines/Formal Verification
- three experimentations (fourth: 5th of Nov. 2006)
- various actions to understand acceptability of the system

... in a (relatively) good position to start assessing benefits and risks of the approach
Outline of the talk

1. The ProVotE project
2. The technological solution
3. Development of the core logic of the machine
4. The trials
5. Conclusions
Part 1.
The ProVotE Project
Initial assumption: introduction of eVoting is multi-faceted problem (technology being just a bit of the problem) and poses several risks

Therefore...

- **Multi-disciplinarity**
  - different competences
  - different roles

- **Multi-phased/Incremental**
  - with emphasis on experimentations and participation
The ProVotE "System"
The ProVotE "System"
The ProVotE "System"
Multi-phased/Incremental

Social research

Prototype’s development

Trials (May 05) (Nov 05) (May 06)

Assessment of Trials

Presentation to Local Council

Tuning and System upgrade

Provincial elections (2008)
Some benefits

- **Interdisciplinarity**
  - Direct participation of the citizens
  - Unique possibility of understanding attitude of citizens towards voting and e-voting
  - Opportunity to help improve participation to (e-)voting by younger people
  - Integration of innovative techniques

- **Multi-phased/Incremental**
  - Minimizes risks (both technological and sociological)
  - Helps refining solution based on user needs
  - Allows for accumulating a significant set of data
Part 2. The Technological Solution
Voting Procedure in Italy
Make or buy...

- Personalization of the system to the local “environment”
- Local solutions thought of as more acceptable than external solutions
- More control over quality of the final product (especially if non profit organizations/research centers are involved in the process)
- Occasion for local development
The overall Architecture
The e-voting machine (1/2)

- VVPAT (each vote gets printed)
- Interaction is touch-screen based
- Identification of the electorate is external to the machine
- Each vote is cut (no sequence in the paper trail)
- Paper trail behind a glass
The e-voting machine (2/2)

- Stand-alone. Getting access to the hardware requires to unlock the cabinet.
- Based on standard technologies (for the trials we reused existing systems).
- Software is Java and Linux Based (Linux stripped to essential services).
- Data are stored redundantly.
- Formal methods techniques used for the "core" logic.
- All sensitive data are encrypted and digitally signed.
- Votes stored in a single file. Votes are shuffled.
Characteristics (1/2)

- DRE w/ VVPAT (touch screen and printer)
- Paper trail behind a glass
- Printer w/ cutter
- Linux (customised) and Java based
- Isolated from the net
- Data stored redundantly
Characteristics (2/2)

- Machine locked by default
- A (machine specific) smartcard unlocks the machine for voting
- A light system helps fulfill the normative requirement (giving every voter the right to express their vote)
e-Voting Interface (1/2)

- Major
- Councillors
- Party
e-Voting Interface
Audit Trail

- 4.5 inches wide
- recounting made possible/efficient in practice by barcode systems
Part 3. Development of the core logic of the voting machine
Motivations

- The voting machine is the most critical component
  - Service Levels
  - Visibility (especially in trials - since you are building trust by the users)
  - Limited control on the environment
- Compliance
  - Behaviour of the machine and electoral processes
- Configurability
  - Different deployments (free simulation, training, voting)
  - Adaptation to different voting rules and laws
(Some) Development Process Choices

- **Compliance ... Traceability**
  - Try and trace the behaviour of the machine back to the norms

- **Configurability ... Flexibility**
  - FSM based notation both for the control logic and for the GUI specification
  - Tool supported (open source license as a plus)

- **Visibility ... Verifiability**
  - Integration of model checking techniques in the development process
  - Fine control on the compilation and compilation steps
Model Checking

- **Basic Ingredients**
  - System Modeled as a Finite State Automata
  - Properties Expressed in Temporal Logic
  - Formal V&V by exhaustive search over the state space

- **Model Checking Tool**

  ![Diagram](image.png)

  - Property
  - FSA
  - NuSMV
  - Yes
  - Counterexample
jProVotE Architecture
jProVotE Architecture
Development Process
FSMC+: Support Tools

Ingredients...

UML Statecharts
XMI, SMC,
Code Generation, Model Checking
The NuSMV Model Checker

NuSMV is an Industrial Strength, Open Architecture, Model Checker

- Joint project with CMU
- Academic version released in June 99
- Over 200 installations worldwide
- High quality implementation
- Interest by various industrial partners (e.g. Boeing)

... and it is open-source
Hypotheses

- Support for a subset of the Statechart notation

- Relatively simple computational model (driven by the application and applicative domain)
UML Modeling Tool
Part 3. The Trials
3 trials

20 precincts

8500 voters

7 municipalities

Trento Fondo Coredo

Lomaso Baselga di Pinè

Daiano Peio
The Trials

- **Characteristics**
  - On a (relatively) small scale (as elections allowed)
  - With experimental value
  - Municipalities chosen by Sociology
  - Machines in the precincts operated by precinct personnel (after a half-a-day training session)
  - Voters on an voluntary basis
  - Volunteers asked to repeat their vote

- **Approach**
  - Standardize, Delegate, and Measure
Standardise...

- **Standard calendar and standard set of actions**
  - Public meetings
  - Information campaign (videos, systems available for testing)
  - ...

- **Standard set of material**
  - Communication kit
  - Training kit
  - ...
... Delegate ...

... some obvious:

- Operation of the machines during the electoral day
  - in smaller places helps increase participation ("chain" of trust)
  - from the technological point of view, only way of setting equipment in a real environment

... and some maybe less obvious:

- Information and communication campaign
... Measure

- Sociological measures before, during, and after the experimentations
  - Focus groups
  - Phone interviews
  - Interviews during the election day
  - Follow up interviews months after the trials

- Technological measures during and after the elections
  - Verification of audit trails/electronic results
  - Log analysis (monitored and validated by the Electoral Service)
Results

At the "object" level

- Electronic elections anticipated the results of the paper election in all cases
- Manual recount always matched the electronic results (thought as obvious when we started the project, not so obvious after you get to know about other experiences)

At the "meta" level

- Attitude of Trentino's towards new technologies
- Novel insights on the behavior of the electorate
- Excellent insight on procedures, guidelines and indications for large scale introduction
What Voters Think

- Easy to use: 7.9 (Electronic), 7.9 (Paper)
- Fast: 8.9 (Electronic), 7.8 (Paper)
- Secrecy: 7.6 (Electronic), 7.4 (Paper)
- Fewer costs (less personnel): 7.9 (Electronic), 7.1 (Paper)
- Fast results: 7.8 (Electronic), 6.9 (Paper)
- More difficult to alter data: 6.9 (Electronic), 6.8 (Paper)
- Easy to interpret: 6.4 (Electronic), 5.4 (Paper)

Comparative analysis of electronic and paper voting systems.
Part 4. Conclusions
Conclusions

- **Key factors in success sofar:**
  - Inter-disciplinarity
  - Participation by citizens
  - Involvement of Public research centers

- **Some (technological) lesson learned:**
  - Perceived security versus actual security
    - need for negotiating/communicating with the stakeholders choices in the system
  - Process is as important as systems
    - security results from a combination of both
  - Need/opportunity for standardization
    - make different solutions interoperable
Future Work
Security in the Environment
Support Tools

Analisi sul modello

Documentazione Matrice CRUD Responsabilità di processo

Responsabilità su entità Analisi di sicurezza
Support Tools
Appendix
E-voting: attitudes - I

Voting procedures should be changed, sooner or later (70%)
E-voting is a good idea, but it is difficult to implement (58%)

Should e-voting be adopted in the next provincial elections, would you be...

- in favour 37%
- very in favour 19%
- indifferent 19%
- against 11%
- very against 11%
- no answer 3%

n=2561
## Attendance in elections:

<table>
<thead>
<tr>
<th></th>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very in favour</td>
<td>20,0</td>
<td>12,5</td>
<td>13,8</td>
</tr>
<tr>
<td>Quite in favour</td>
<td>37,1</td>
<td>27,1</td>
<td>17,2</td>
</tr>
<tr>
<td>Indifferent</td>
<td>17,3</td>
<td>34,0</td>
<td>51,7</td>
</tr>
<tr>
<td>Against</td>
<td>11,8</td>
<td>9,0</td>
<td>3,4</td>
</tr>
<tr>
<td>Very against</td>
<td>11,2</td>
<td>13,2</td>
<td>8,6</td>
</tr>
<tr>
<td>No answer</td>
<td>2,7</td>
<td>4,2</td>
<td>5,2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>%</th>
<th>100,0</th>
<th>100,0</th>
<th>100,0</th>
</tr>
</thead>
</table>

\[ N = 2347 \]
E-voting: attitudes - III

Professionals, students, highly educated, below 50

>65%

% agreement (average: 56%)

<40%

Retired, elderly, no education

Size and level of development of a town have no effect

Education impacts only if it is very low, controlling for age and technological skills
E-voting: attitudes - IV

WHAT MATTERS is: a positive or negative attitude

Belief that e-vote will:
- Limit contentions
- Lower mistakes
- Increase frauds
- Increase abstentions

And (hypothesis):
- Feeling voting as a duty
- Feeling confident of own skills
- Trust institutions
After the trials - II

- Telephone interviewing four months after the first trial
- The sample is representative of the adult population in the electoral sections that experimented e-voting

<table>
<thead>
<tr>
<th></th>
<th>sample</th>
<th>testers</th>
<th>watchers</th>
<th>non-voters</th>
</tr>
</thead>
<tbody>
<tr>
<td>very in favour</td>
<td>21%</td>
<td>32%</td>
<td>12%</td>
<td>9%</td>
</tr>
<tr>
<td>in favour</td>
<td>41%</td>
<td>49%</td>
<td>39%</td>
<td>28%</td>
</tr>
<tr>
<td>indifferent</td>
<td>17%</td>
<td>8%</td>
<td>20%</td>
<td>36%</td>
</tr>
<tr>
<td>against</td>
<td>14%</td>
<td>9%</td>
<td>19%</td>
<td>12%</td>
</tr>
<tr>
<td>very against</td>
<td>7%</td>
<td>2%</td>
<td>10%</td>
<td>14%</td>
</tr>
<tr>
<td><strong>N</strong></td>
<td><strong>1206</strong></td>
<td><strong>503</strong></td>
<td><strong>372</strong></td>
<td><strong>146</strong></td>
</tr>
</tbody>
</table>
Questions?

Roberto Tiella
ITC-irst
tiella@irst.itc.it

Adolfo Villafiorita
ITC-irst
adolfo@irst.itc.it

Silvia Tomasi
ITC-irst
silviadik@tin.it