# 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

CSDUML06
Genova
Oct 1 2006

ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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)



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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.”*



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Context: eVoting in Trentino

Provincial Law, 5/3/2003, n. 2, *"Norme per l'elezione diretta del Consiglio provinciale di Trento e del Presidente della Provincia"*

**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.



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# ProVotE: Goal of the Project

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 astensionism

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



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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**



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Part 1.
# The ProVotE Project

CSDUML06
Genova
Oct 1 2006

ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Approach

**Initial assumption:** introduction of eVoting is multi-faceted problem (technology being just a bit of the problem) and poses several risks

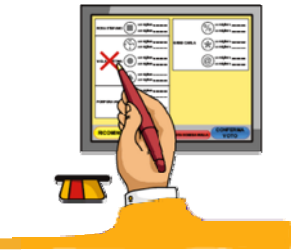
Therefore...

- **Multi-disciplinarity**
  - different competences
  - different roles
- **Multi-phased/Incremental**
  - with emphasis on experimentations and participation



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The ProVotE "System"



PROVINCIA AUTONOMA DI TRENTO

REGIONE AUTONOMA TRENTINO/ALTO-ADIGE

CONSORZIO DEI COMUNI TRENTINI
SEZIONE SCUOLA E FORMAZIONE

ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

COMUNE DI TRENTO

UNIVERSITÀ DEGLI STUDI DI TRENTO

GraphiTech

IPRASE TRENTINO

Informatica Trentina SpA

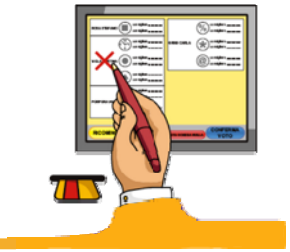
Citizens

Students



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The ProVotE "System"



PROVINCIA AUTONOMA DI TRENTO

REGIONE AUTONOMA TRENTINO/ALTO-ADIGE

COMUNE DI TRENTO

UNIVERSITÀ DEGLI STUDI DI TRENTO

ITC irst

GraphiTech

IPRASE TRENTINO

Informatica Trentina SpA

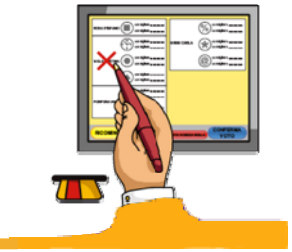
Citizens

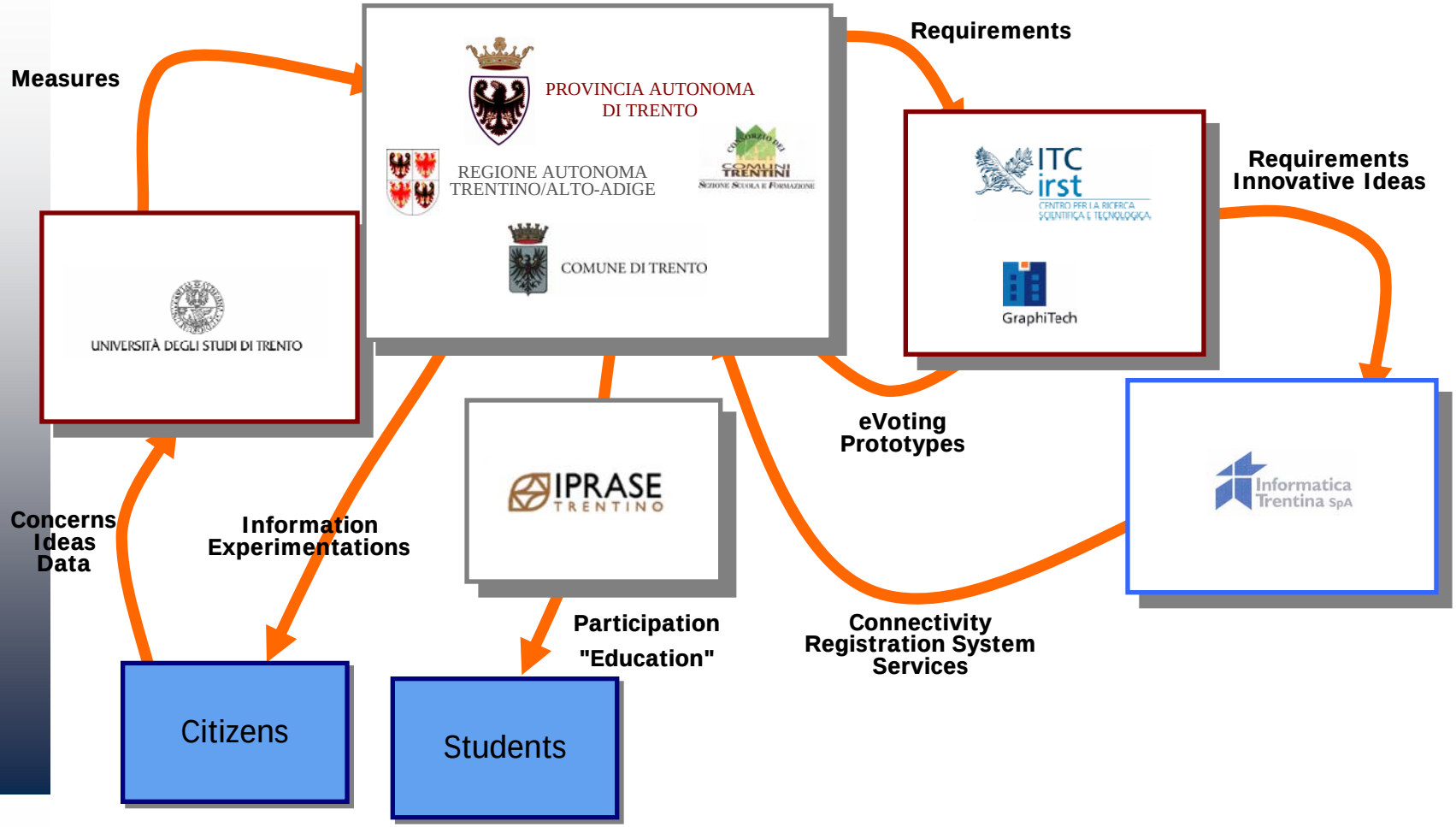
Students



ITC irst

# The ProVotE "System"

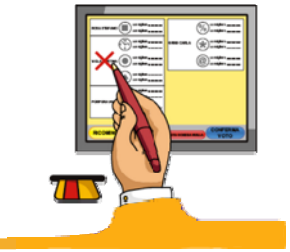


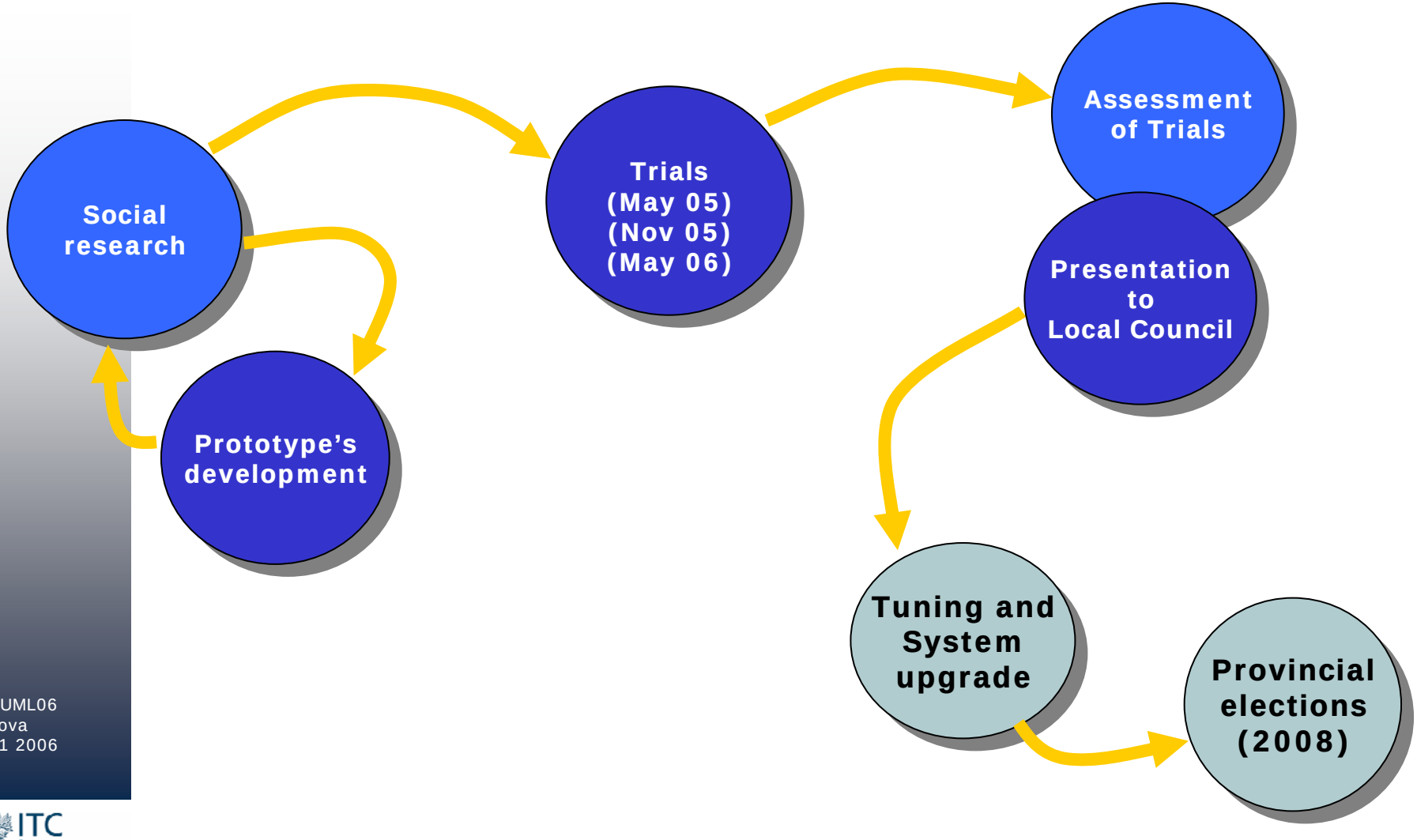





ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Multi-phased/Incremental








ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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



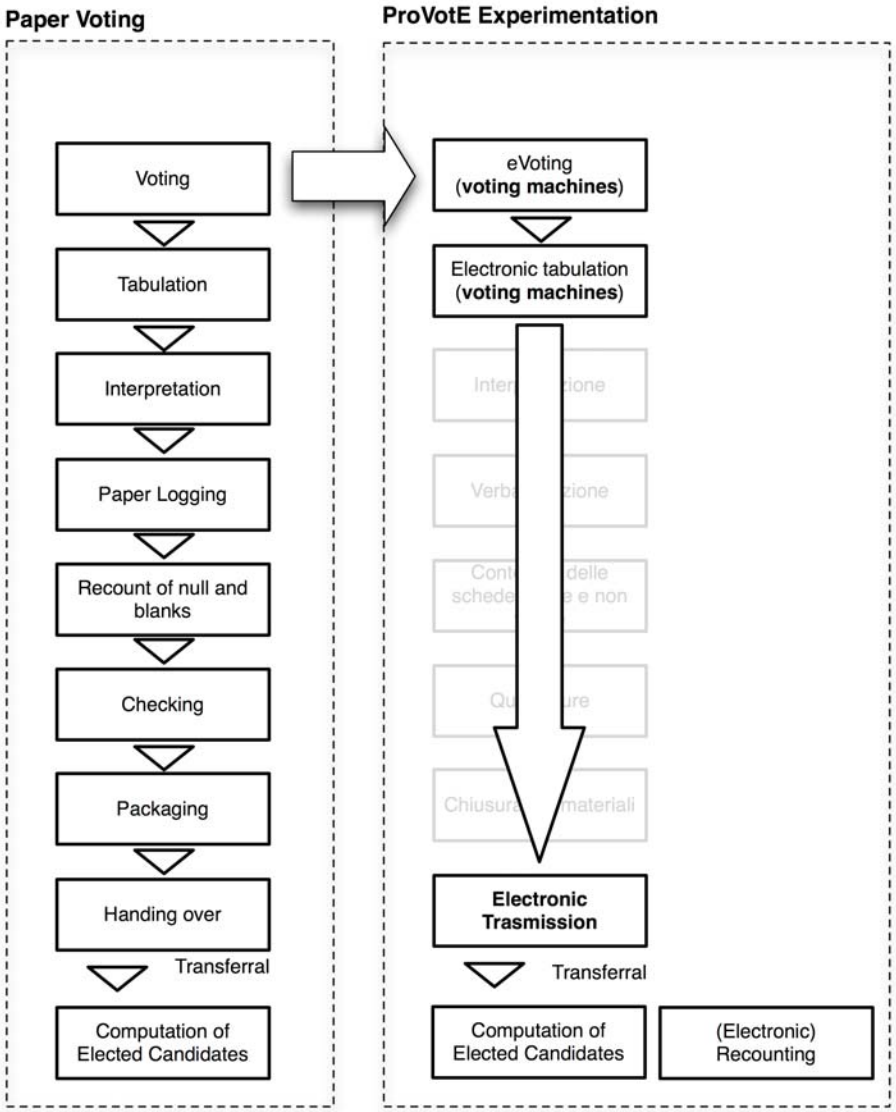
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Part 2. The Technological Solution



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

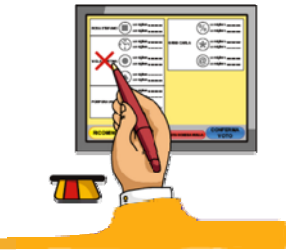
# Voting Procedure in Italy






ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Make or buy...

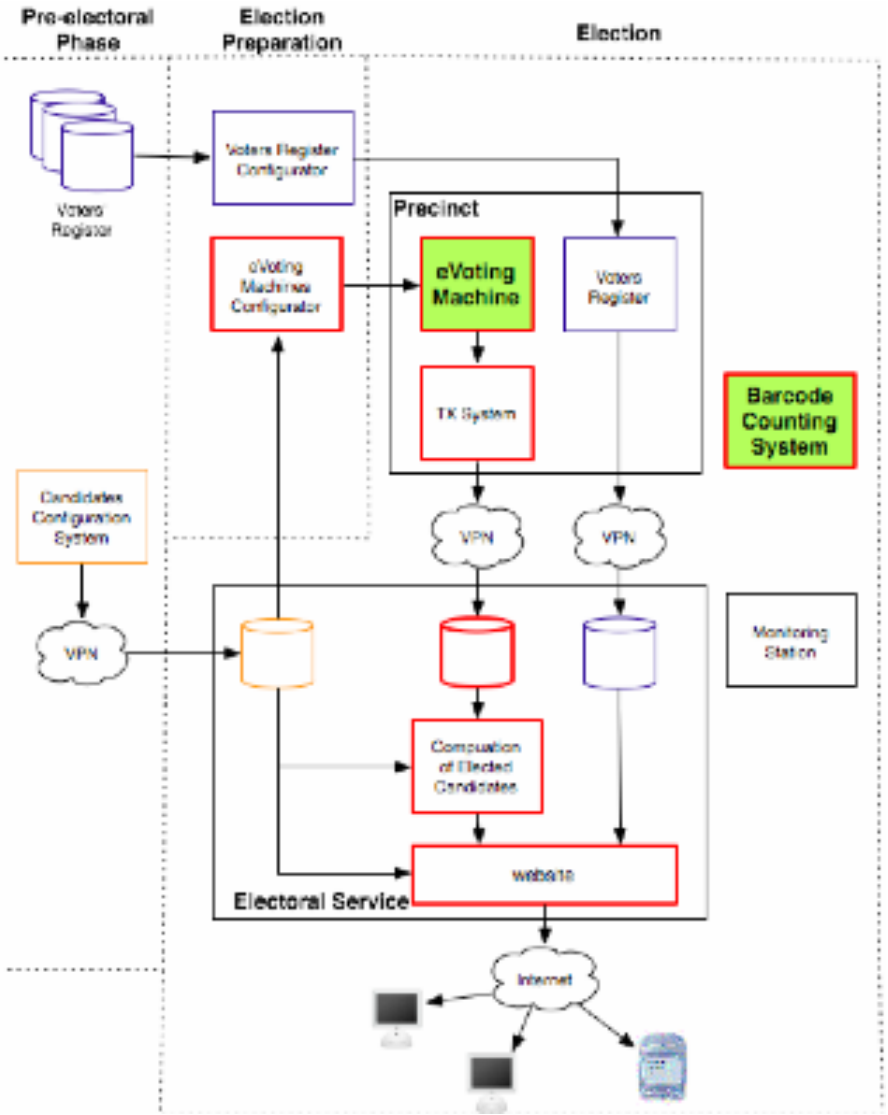


- Personalization of the system to the local "environment"
- Local solutions thought of as more acceptable than external solutions
- More control over quality of the final product (especially if non profit organizations/research centers are involved in the process)
- Occasion for local development



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The overall Architecture






ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The e-voting machine (1/2)

VVPAT (each vote gets printed)

Interaction is touch-screen based

Each vote is cut (no sequence in the paper trail)

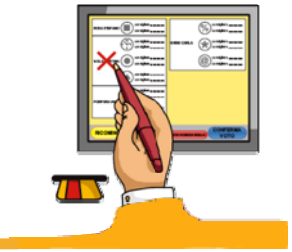
Paper trail behind a glass

Identification of the electorate is external to the machine



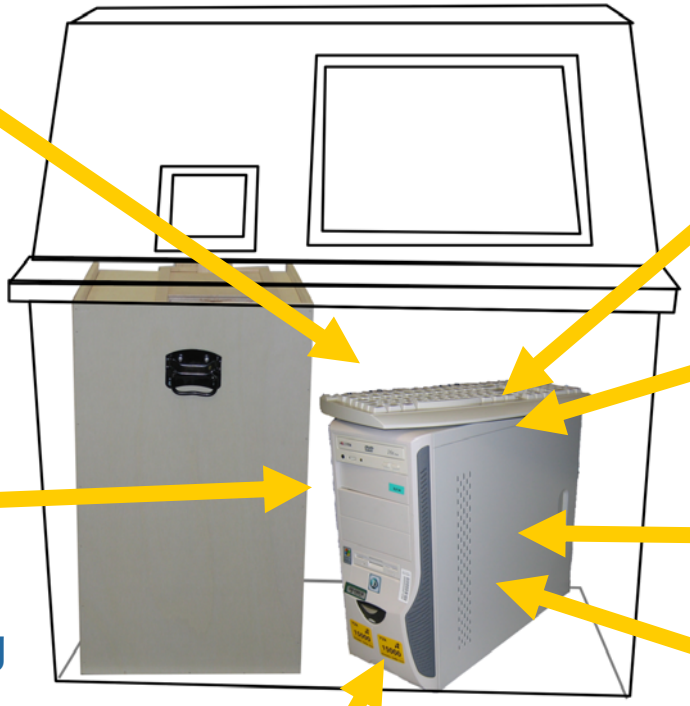
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The e-voting machine (2/2)



Based on standard technologies (for the trials we reused existing systems)

Software is Java and Linux Based (Linux stripped to essential services)



Formal methods techniques used for the "core" logic

Votes stored in a single file. Votes are shuffled.

Stand-alone. Getting access to the hardware requires to unlock the cabinet

Data are stored redundantly

All sensitive data are encrypted and digitally signed

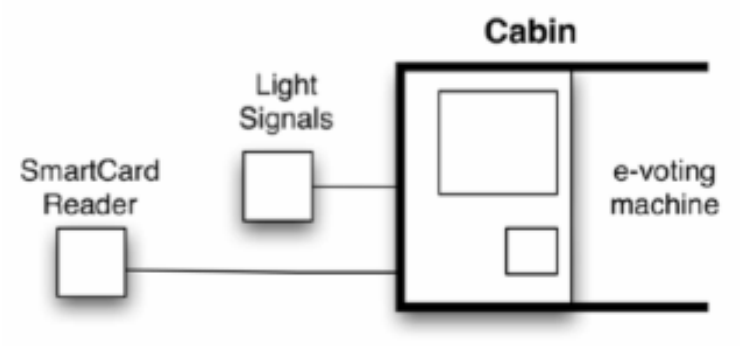


ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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 the express their vote)



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA



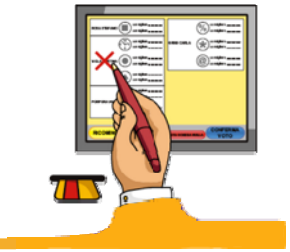
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

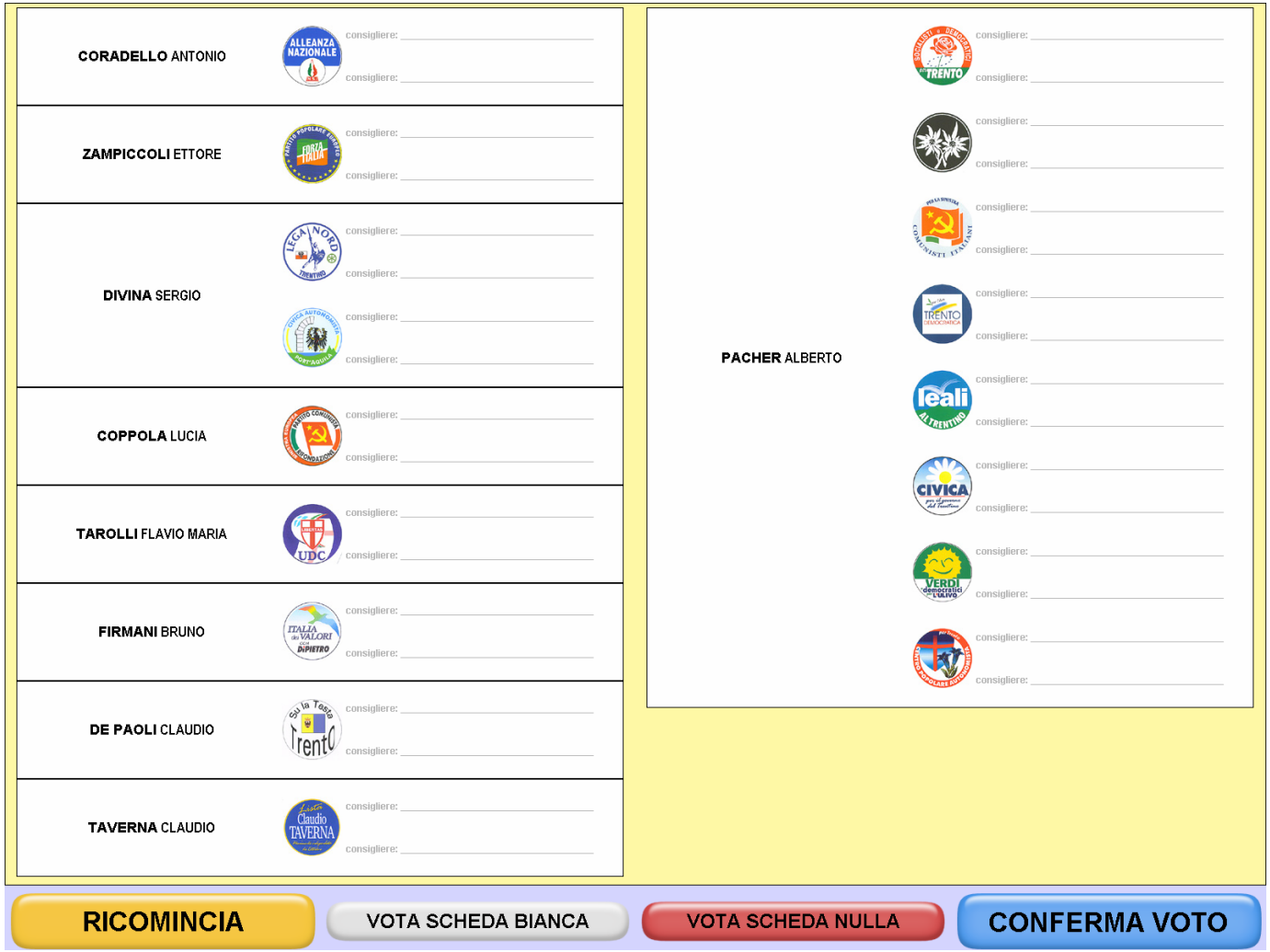
# e-Voting Interface (1/2)




ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# e-Voting Interface

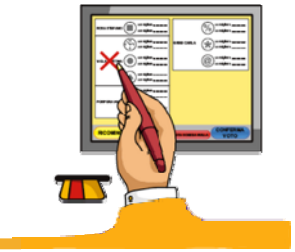





CSDUML06
Genova
Oct 1 2006

ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Audit Trail




**major**

**party**

**councillors**

**"blank"** **"null"**


- 4.5 inches wide
- recounting made possible/efficient in practice by barcode systems



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Part 3. Development of the core logic of the voting machine



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

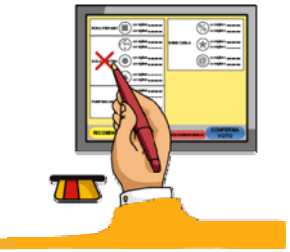
# (Some) Development Process Choices

- **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

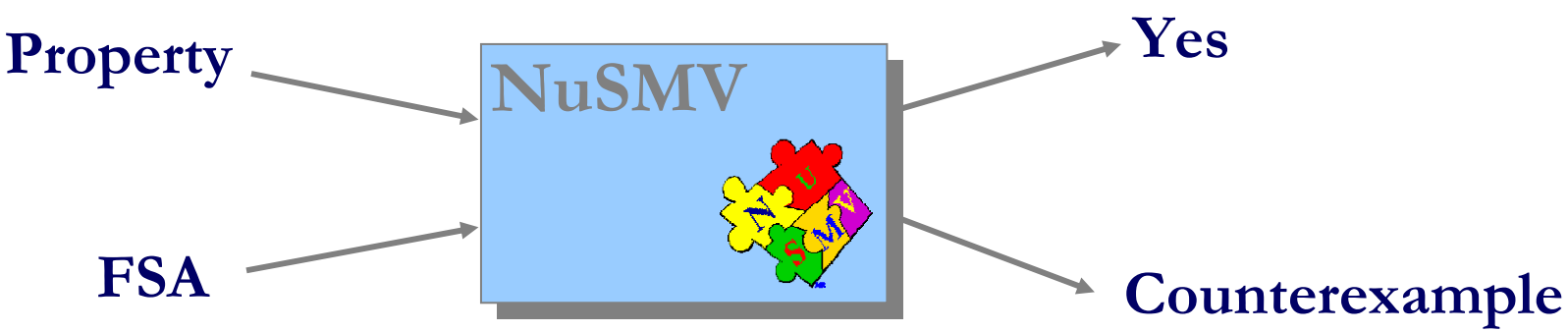


ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

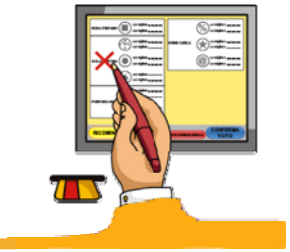
# Model Checking

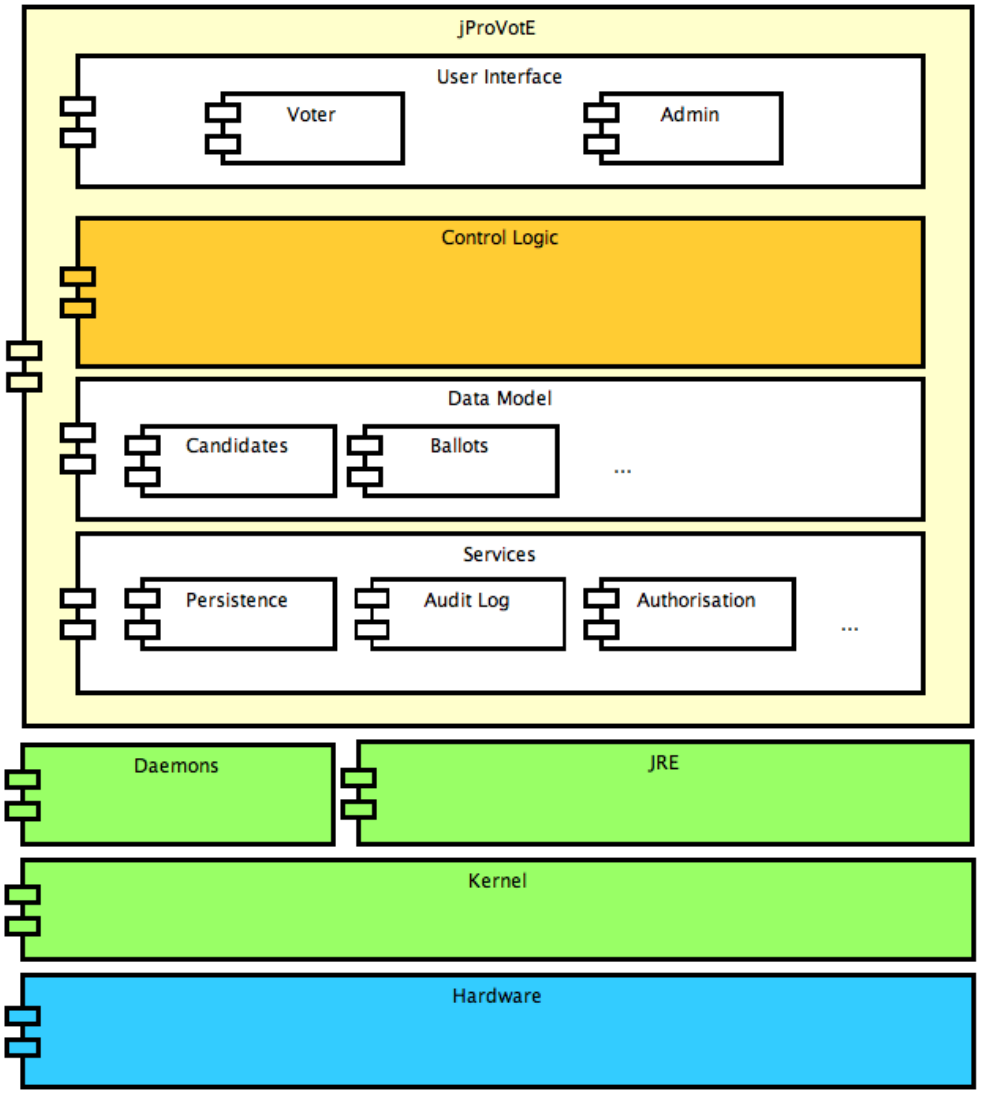


- **Basic Ingredients**
  - System Modeled as a Finite State Automata
  - Properties Expressed in Temporal Logic
  - Formal V&V by exhaustive search over the state space
- **Model Checking Tool**



# jProVotE Architecture

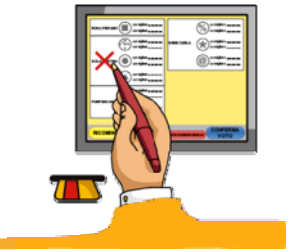


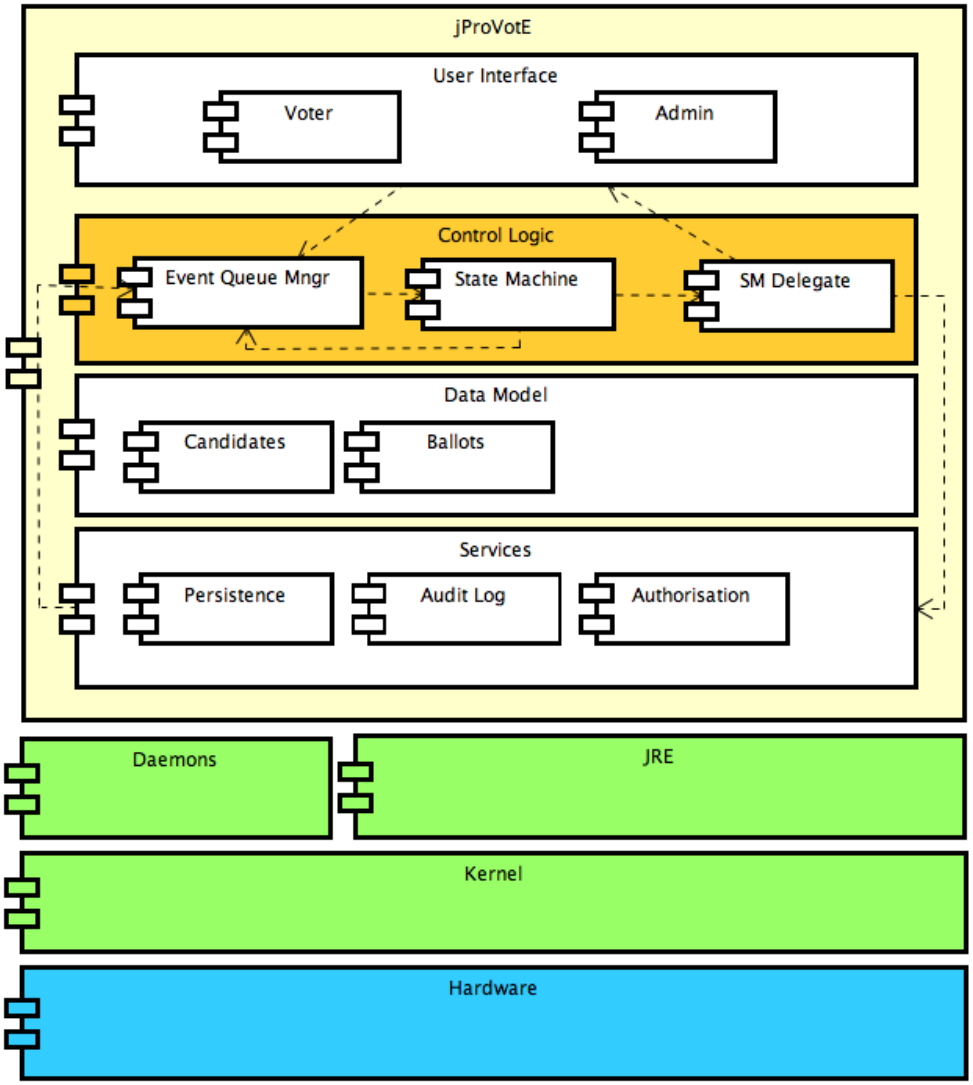





ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# jProVotE Architecture

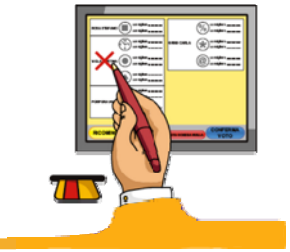


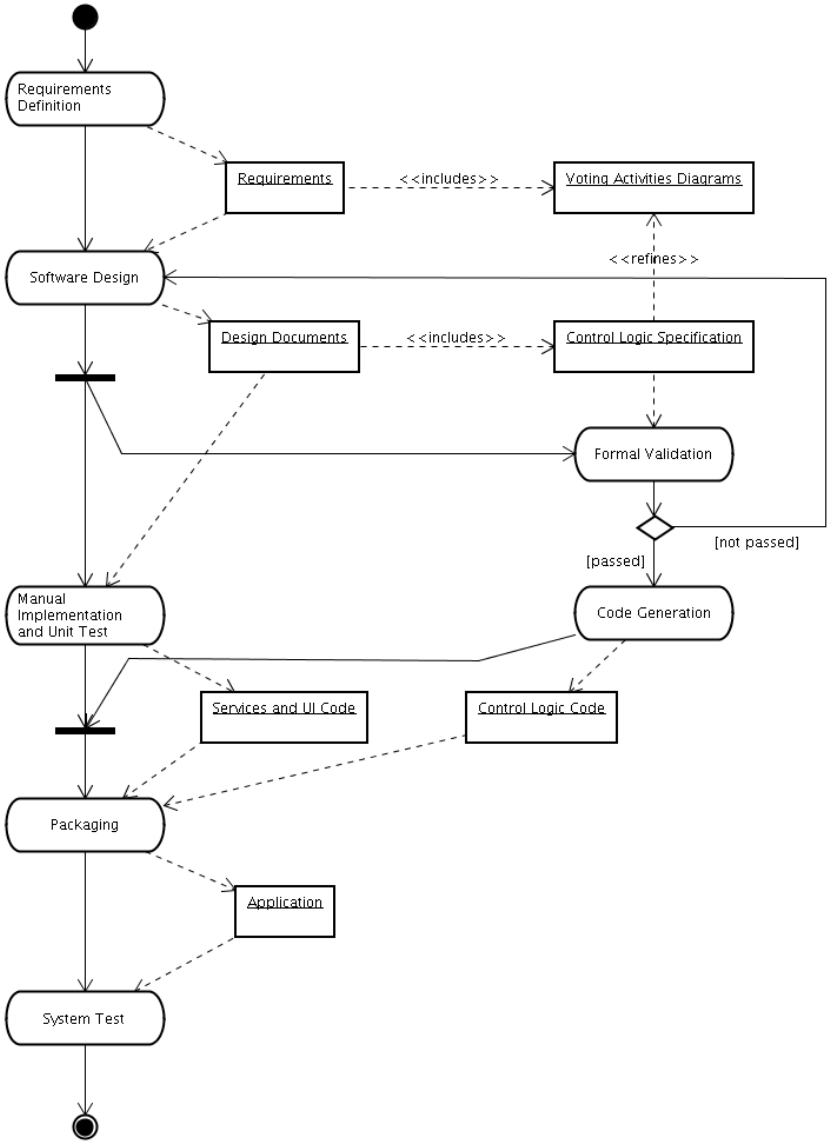





ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Development Process

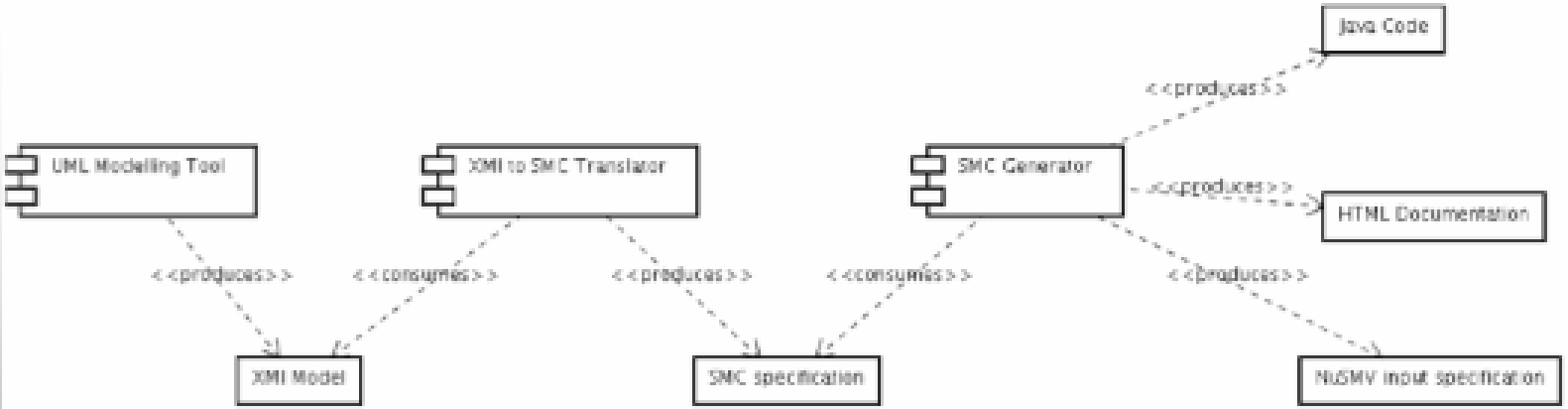







ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# FSMC+: Support Tools




Ingredients...

**UML Statecharts**

**XMI, SMC,**

**Code Generation, Model Checking**



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# The NuSMV Model Checker

## NuSMV is an Industrial Strength, Open Architecture, Model Checker

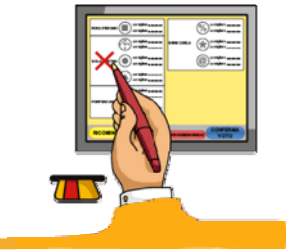
- Joint project with CMU
- Academic version released in June 99
- Over 200 installations worldwide
- High quality implementation
- Interest by various industrial partners (e.g. Boeing)

**... and it is open-source**

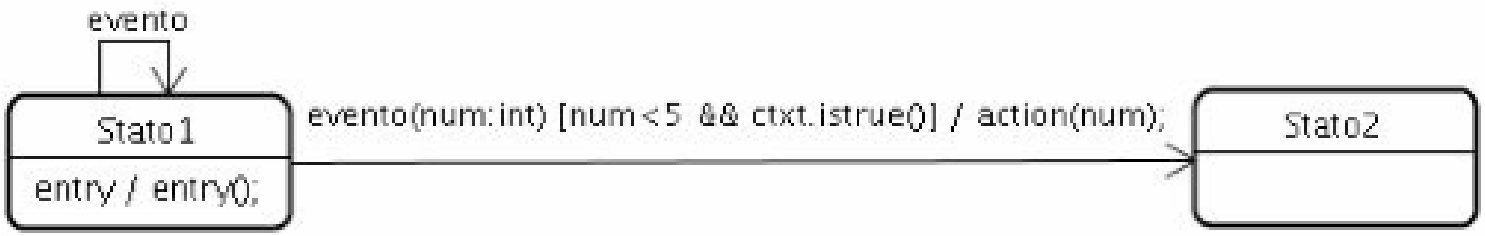


ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Hypotheses

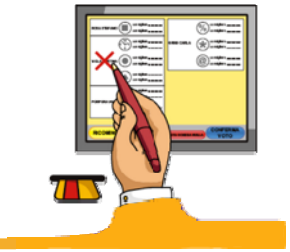


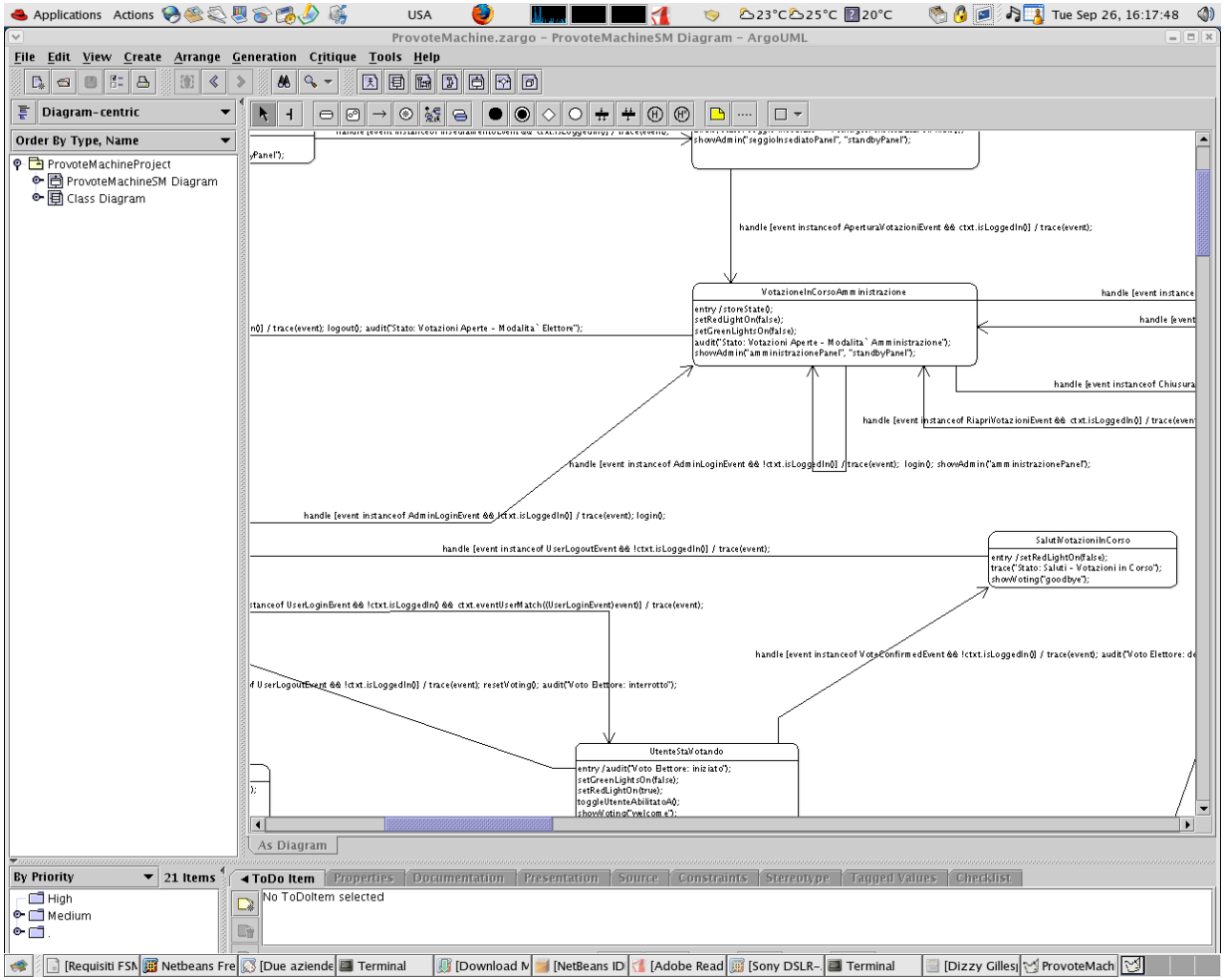
- Support for a subset of the Statechart notation




- Relatively simple computational model (driven by the application and applicative domain)

# UML Modeling Tool






CSDUML06
Genova
Oct 1 2006

ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Part 3. The Trials



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 3 trials

8 may 2005

6 nov 2005

28 may 2006

## 20 precincts

# 8500 voters

## 7 municipalities

Trento Fondo Coredo

Lomaso Baselga di Pinè

Daiano Peio



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

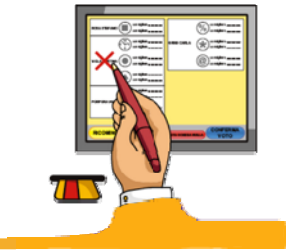
# The Trials

- **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



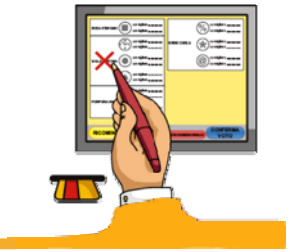
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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)

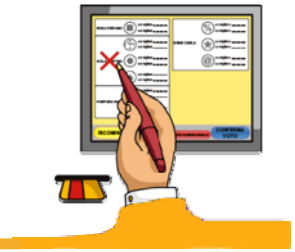
## At the "meta" level

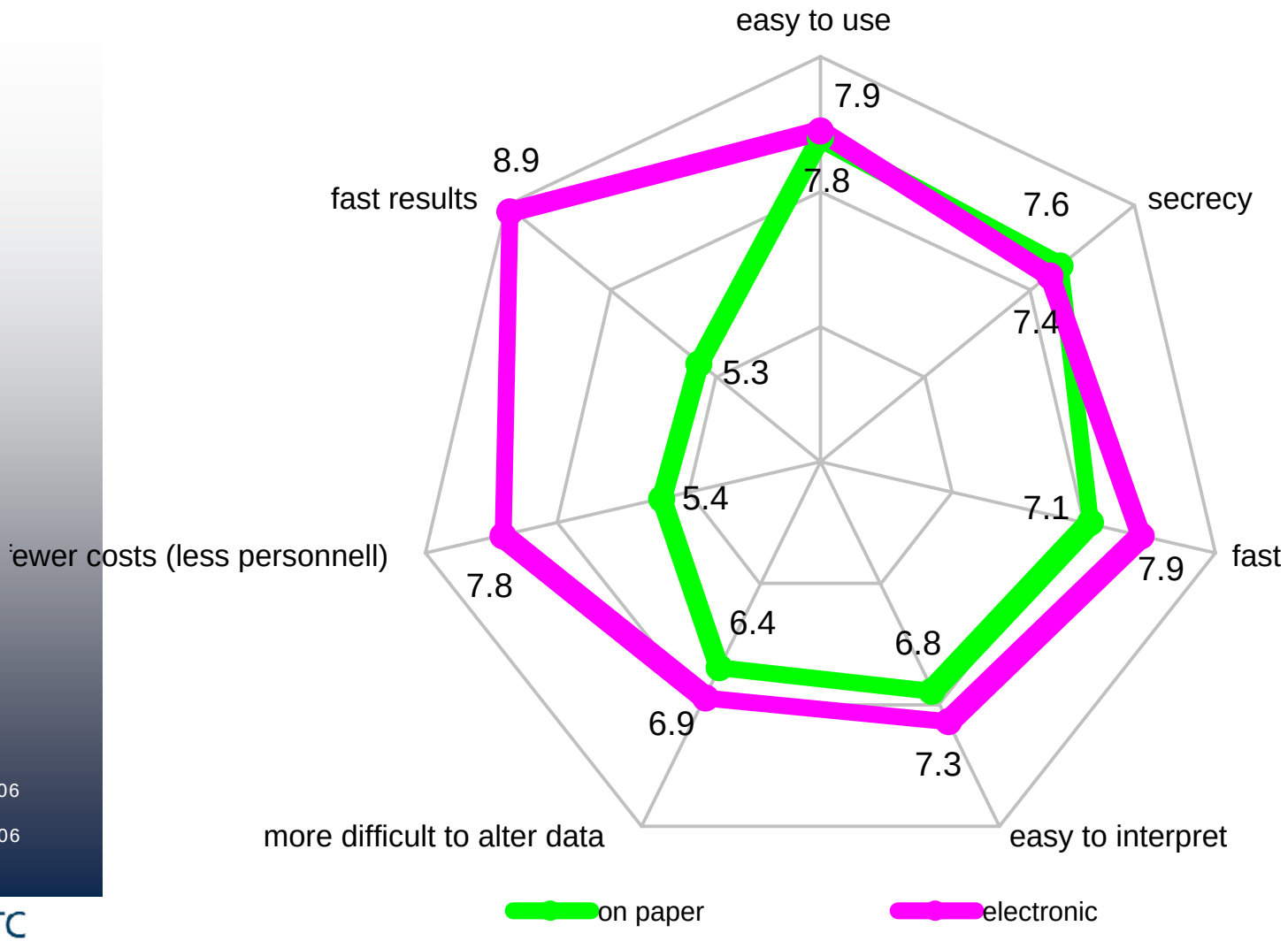
- Attitude of Trentino's towards new technologies
- Novel insights on the behavior of the electorate
- Excellent insight on procedures, guidelines and indications for large scale introduction



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# What Voters Think








ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Part 4. Conclusions



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

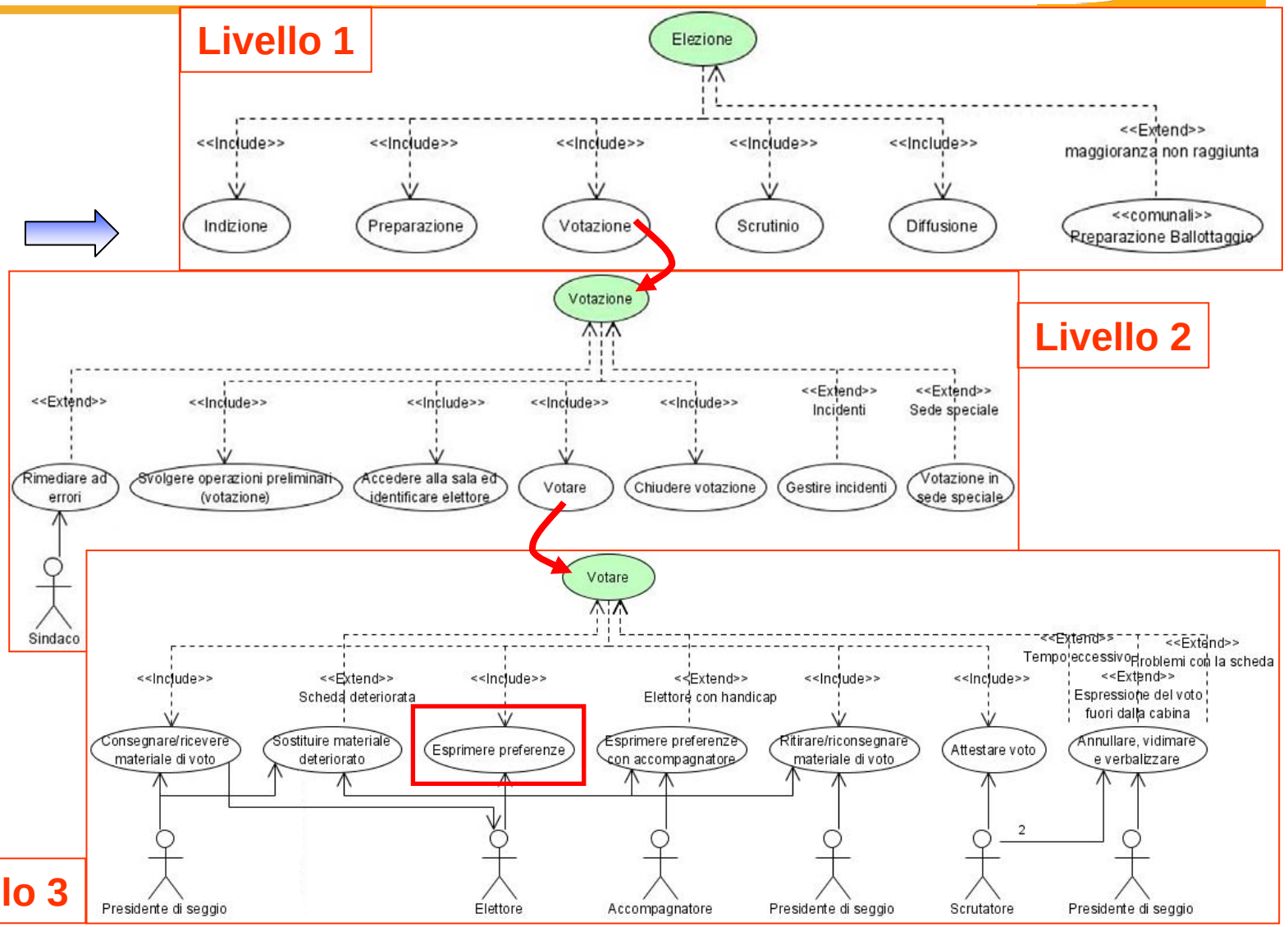
# Future Work



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Security in the Environment

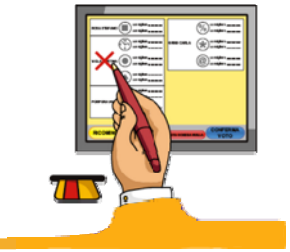


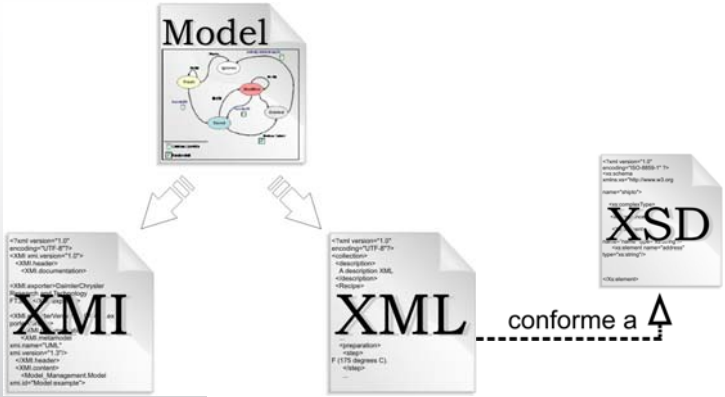



Oct 1 2006

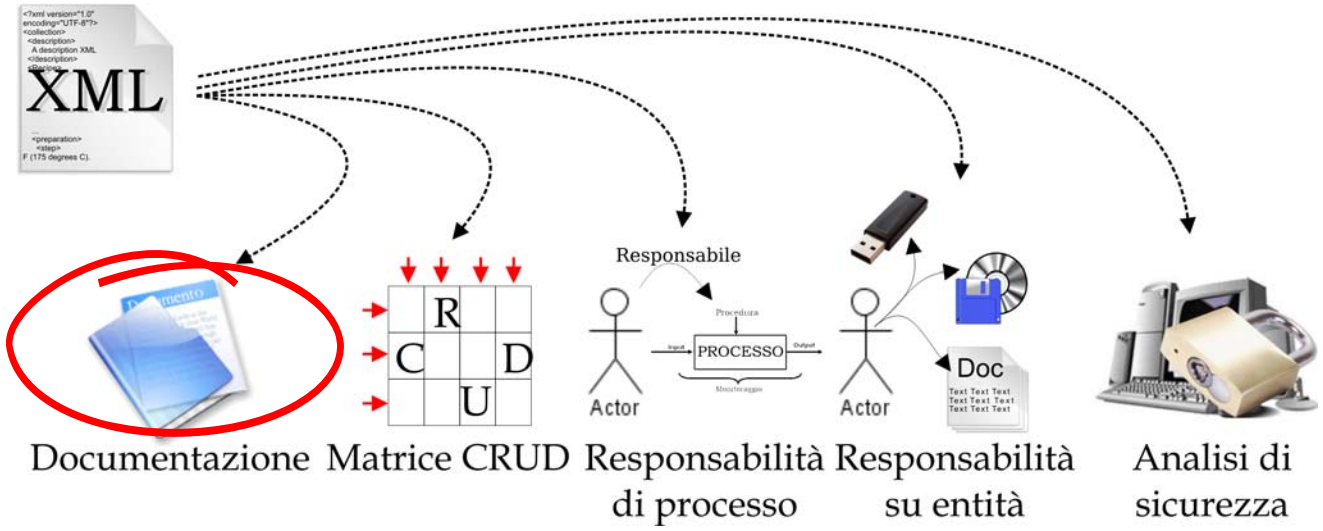
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Support Tools

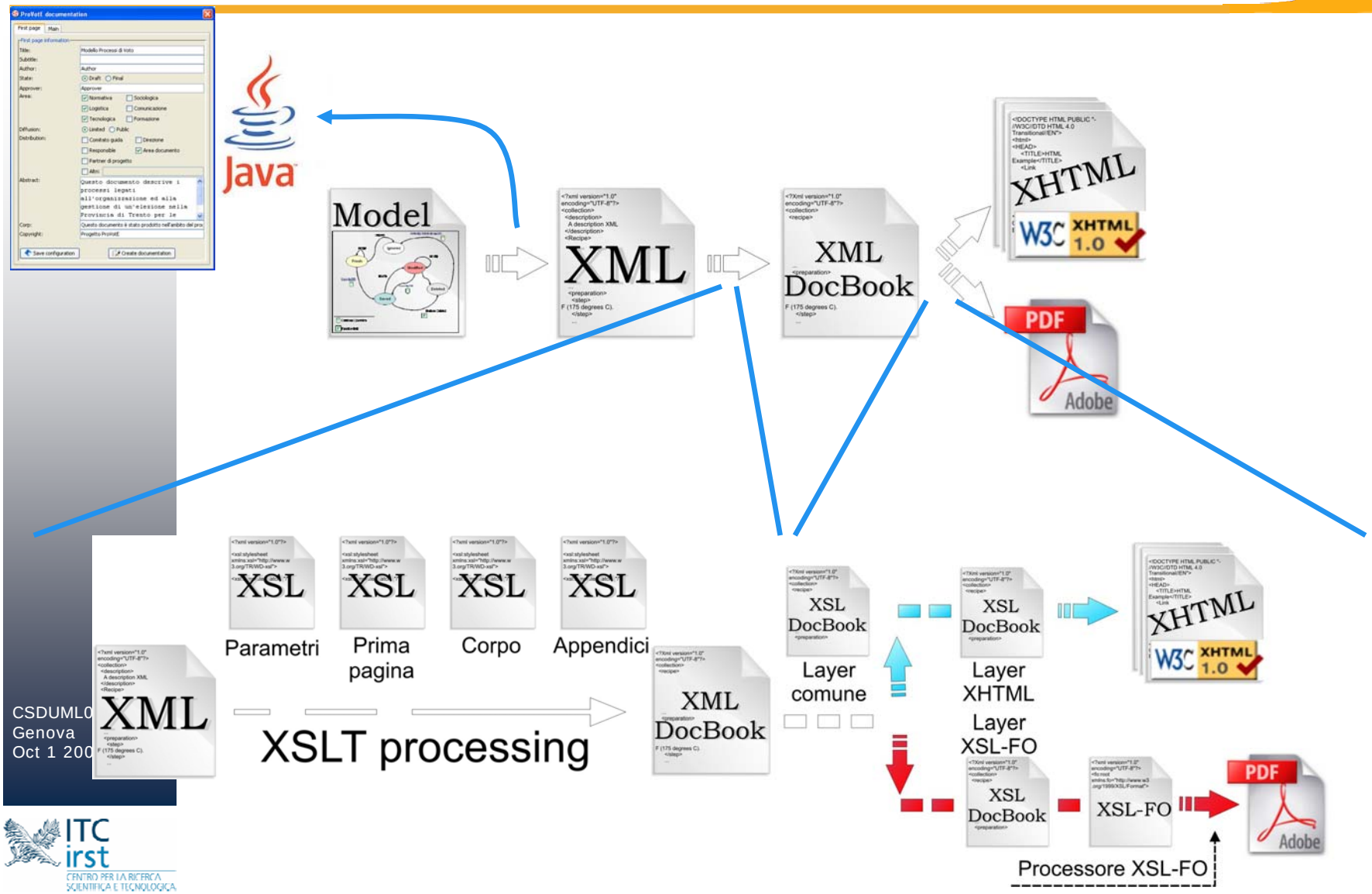





**Analisi sul modello**



# Support Tools






ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Appendix



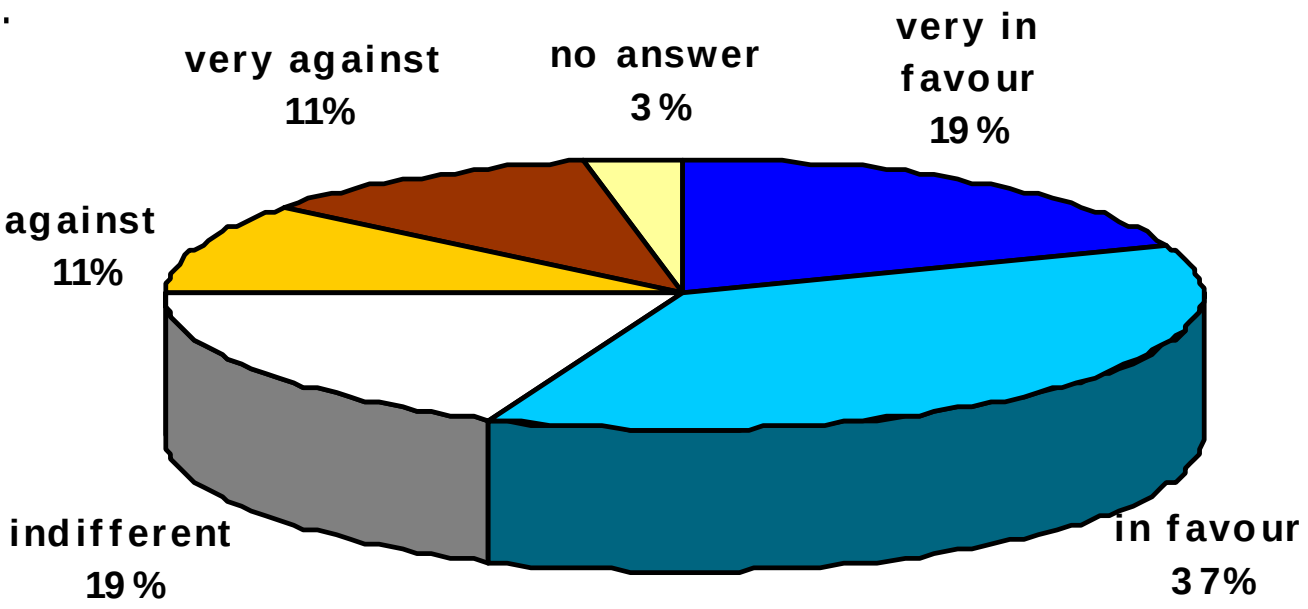
ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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…




*n=2561*

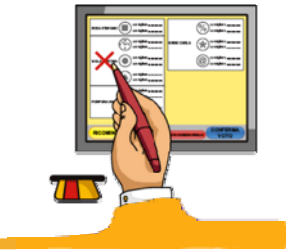


ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# E-voting: attitudes - II

| *Attendance in elections:* | ***Always*** | ***Sometimes*** | ***Never*** |
|---|---|---|---|
| **Very in favour** | 20,0 | 12,5 | 13,8 |
| **Quite in favour** | 37,1 | 27,1 | 17,2 |
| **Indifferent** | 17,3 | 34,0 | 51,7 |
| **Against** | 11,8 | 9,0 | 3,4 |
| **Very against** | 11,2 | 13,2 | 8,6 |
| **No answer** | 2,7 | 4,2 | 5,2 |
| *%* | 100,0 | 100,0 | 100,0 |
| *N =* | *2347* | *144* | *58* |

# E-voting: attitudes - III



Professionals, students, highly educated, below 50

**>65%**

*% agreement (average: 56%)*

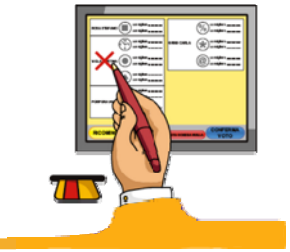
**<40%**

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 | Increase frauds |
| Lower mistakes | Increase abstentions |

feeling voting as a duty

feeling confident of own skills

*And (hypothesis):* trust institutions



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# 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

| | ***sample*** | testers | watchers | non-voters |
|---|---|---|---|---|
| very in favour | ***21%*** | 32% | 12% | 9% |
| in favour | ***41%*** | 49% | 39% | 28% |
| indifferent | ***17%*** | 8% | 20% | 36% |
| against | ***14%*** | 9% | 19% | 12% |
| very against | ***7%*** | 2% | 10% | 14% |
| *N* | ***1206*** | *503* | *372* | *146* |



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA

# Questions?

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

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

**Silvia Tomasi**
ITC-irst
silviadik@tin.it



ITC irst
CENTRO PER LA RICERCA SCIENTIFICA E TECNOLOGICA