
Mark Phillips & Richard Soudriette
Grüße aus Richard Soudriette!

“Ohne Demokratie gibt es keine Freiheit.”

Friedrich Ebert, President of Germany (1919-1925)
Independent testing provided by an accredited, qualified source, coupled with EMB certification are essential tools for voting system performance and public confidence.

- Technology Challenges
- Need for accepted international standards
- Voting system testing framework
- Case Studies
Before Ballots - *The County Election*
Lever Machines “..Make the process of casting the ballot perfectly plain, simple and secret”
Technology Complexity and Testing Challenges
Lack of Transparency Leads to Distrust
Need for International Standards

- 2004 Council of Europe e-voting standards focused on reliable auditing and certification
- 2010, Council of Europe *The E-Voting Handbook*, encourages independent testing and certification of e-voting systems
- 2005 US VVSG
- Many individual standards issued by other countries and jurisdictions
Carter Center Report on 2006 Venezuelan Elections

“Impartial, independent, and transparent system certification measures should be in place to insure that the system meets national or international standards, the requirements of the elections jurisdiction, as well as the technological specifications outlined by the vendor.”
Electronic Voting System Test Framework

Testing body should be a credentialed, independent test lab with specific expertise in voting systems and proven test methods to ensure voting systems are:

- **Secure**
  - Protect against unauthorized manipulation; establish controls to minimize errors; identify erroneous changes; protect secrecy

- **Accurate**
  - Capture, record, store, and report ballot selections without error

- **Reliable**
  - Guard against improper information modification; ensure information non-repudiation and authenticity

- **Audit-able**
  - Record information in a way that it can be audited to verify steps followed without compromising voter secrecy
<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
<th>Phase 6</th>
<th>Phase 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver/Receive Vendor Package</td>
<td>TDP Deliverable Check-In</td>
<td>Readiness Test</td>
<td>Vendor Specific Module Creation</td>
<td>Trusted Build</td>
<td>Official Test Execution</td>
<td>Test Report</td>
</tr>
<tr>
<td>Test Suite Development</td>
<td>Training</td>
<td>Readiness testing continues through Phase 4 and must be completed prior to the start of Phase 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Receive Equipment/Voting Materials</td>
<td>HW Configuration Audit</td>
<td>Set-Up Test Equipment Check-In and Operational Status Check</td>
<td>Develop HW Test Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard</td>
<td>HW Test Execution</td>
<td>Test Plan Development continues throughout the testing lifecycle and is completed at the end of Phase 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual/Automated Source Code Review</td>
<td>Manual/Automated Source Code Review continues through Phase 3 and must be completed prior to the start of Phase 4. As discrepancies are uncovered during Phases 4-5, additional Source Code Review may be required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HW testing continues through Phase 3 and must be completed prior to the start of Phase 4. Should HW issues be found during Phases 4-5, additional HW testing may be required.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Return Equipment to Vendor</td>
<td>Archive Test Materials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security

- Physical, Access Control, Software, Data Transmission and Telecommunications

- Validating these areas require specific expertise to ensure the testing is done properly
Accuracy

- Verify that the system accurately conducts and reports the results of all election types used.
- Verify accuracy of the system in less than ideal situations.
- Jurisdictional requirements often call for accuracy testing based on specific election definition.
System Integrity

- Validating the integrity of the voting system to ensure its ability to withstand any data modification or deletion
- Verify that appropriate checks and non-repudiation mechanisms are in place
- Audit-ability provides re-assurance that anything and everything done within the election framework is known and recorded
Documentation

- Documentation review is very detailed and can be a cost driver
- A jurisdiction that maintains equipment itself may need more detail than a jurisdiction that plans to use outside support
- Election officials that anticipate creating election definitions themselves should look for documentation that clearly defines and illustrates the mechanics of the election management system
Source Code Review

- The ability to perform source code review requires a rigorous approach as well as knowledge of tools best suited for the purpose; “other duties as assigned” for development staff rarely yield reliable results.

- Automated as well as manual review with a focus on system security is required.
Automated Source Code Review

- **Identify** the root cause of software security vulnerabilities in both source code (static analysis) and running applications (dynamic analysis)
- **Detect** vulnerabilities across all development languages and APIs
- **Fix** critical security issues faster with collaborative remediation
- **Contain** existing vulnerabilities in deployed software so they can do no harm
- **Govern** the process for ensuring the security of the software
- **Stay** ahead of threats through continuing research on application security issues and threats
- **Comply** with government and industry compliance mandates and internal policies such as Payment Card Industry Data Security Standards (PCI DSS), the Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and North American Electric Reliability Corporation (NERC) standards.
Case Study

- 92 million people, 7,000 Islands
- The name *Philippines* is derived from that of King Philip II of Spain
- In 2007, because of accusations of electoral fraud in electoral processes over the past 4 decades, the Commission on Elections in the Philippines (COMELEC) initiated a nationwide program to automate the electoral process for the 2010 presidential elections.
- With the support of the Congress, funding was provided for implementation of the first nationwide election conducted with optical mark reading equipment with the goal to increase transparency and credibility of the electoral process.
- A key element of the COMELEC’s automated election system for the 2010 presidential elections effort was a vigorous independent testing and certification program.
Republic Act No. 9369
“AN ACT AUTHORIZING THE COMMISSION ON ELECTIONS TO USE AN AUTOMATED ELECTION SYSTEM IN THE NATIONAL OR LOCAL ELECTIONS.. TO ENCOURAGE TRANSPARENCY, CREDIBILITY, FAIRNESS AND ACCURACY OF ELECTIONS, “

- A key provision of the act required third party, independent testing by an internationally accredited voting system test authority be used to certify the system prior to the election

- Supreme Court Chief Justice Puno :“Full automation will not completely cleanse the dirt in our electoral system. But it is a big forward step which can lead us to the gateway of real democracy where the vote of the people is sacred and supreme"
Scope of the Project

- Deliver the comprehensive testing and audit results required to support a timely go/no go decision for electronic elections.
- Conduct a full certification of a new voting system in six months as opposed to more typical US schedules that range from 1 – 2 years.
- Certify the performance, accuracy and security of the system.
- Full code review, hardware testing, functional testing according to modified VVSG standards.
- Provide transparency to citizen stakeholder and political groups.
Day 1 in Manila
Unique technology aspects of ensuring compliance in a challenging environment
Unique technology aspects of ensuring compliance in a challenging environment
Comelec to hold mock polls, field tests for PCOS

By Anna Valmero

INQUIRER.net

MANILA, Philippines—The Commission on Elections (Comelec) will hold a nationwide mock election in December and conduct five other tests before accepting and deploying the poll machines for the 2010 elections, officials said.
Transferring Custody of the Certified Code to COMELEC
U.S. Embassy Statement on Philippine Elections

- The Embassy of the United States extends warm congratulations to the people of the Philippines for achieving another milestone in their nation’s democratic history with the May 10 elections. Philippine citizens served their nation by volunteering at the polls, exercising their right to vote, and taking every step necessary to ensure all ballots were counted. The Embassy was privileged to send 120 observers across the country to witness Philippine democracy in action. While there are always lessons to be learned, our overwhelming impression is that the Philippines has much to be proud of today.

- We look forward to a smooth transition and, after June 30, to working with the new Philippine government to deepen the friendship and partnership between our two nations, and to advance our common goals for the benefit of the Southeast Asia region and the world.
Summary & Conclusion

- Independent testing and certification of e-voting systems are vital tools to safeguard the sanctity of the ballot box and the integrity of the democratic election process.

- Testing and certification also can reassure citizens, candidates and election stakeholders about the transparency and accuracy of e-voting.

- If voters have confidence in the credibility of e-voting machines, they will trust the results.

- Development of internationally accepted standards, and testing conducted by a qualified & trusted source, will accelerate the acceptance of new technologies in voting.
Contact Information

Mark D Phillips
President & CEO
SLI Global Solutions, Inc.
216 16th Street, Suite 700
Denver CO 80108
(303) 575-6881
mphillips@sliglobalsolutions.com