SysTest Labs Certification: What Went Wrong?

SysTest Labs' source code review found many instances of serious programming errors in Smartmatic's programs that may cause, and actually did cause, execution errors on election day, as evidenced by the PCOS program malfunctioning, the PCOS and CCS allowing transmission of FTS results, and a significant number of tabulation errors in the Comelec's public website. Also, SysTest Labs did not test the election design produced by the EMS and the EED for the actual May 10. 2010 election, but only tested the artificially contrived "toy" data supplied by Comelec. Thus there is no way that SysTest Labs could certify that the AES is operating properly, securely, and accurately in accordance with the provisions of RA-9369 because it did not test the AES as it will be used on election day.

Definition of Terms

"Software certification" and "software testing" are closely related and are oftentimes defined the same way. The International Software Testing Qualifications Board (ISTQB) defines "certification"[1] as "the process of confirming that software complies with its specified requirements", for example, by passing a set of software testing procedures. The Wikipedia defines "software testing"[2] as an "investigation conducted to provide information about the quality of the software under test. Software test techniques include, but are not limited to, the process of executing the program or application with the intent of finding software bugs. Software testing can also be stated as the process of validating and verifying that a software program [a] meets the business and technical requirements that guided its design and development, and [b] works as expected".

In this paper, we shall use the definition of "software certification" as the process of validating and verifying that a software program meets the business and technical requirements of the buyer of the software license, Comelec, and works as expected by correctly implementing the election laws of the Philippines and implementing rules and regulations. Software certification may involve the use of various software testing techniques, like executing the program using various sets of input data that will stretch the capabilities of the program to the limit, and determining if anything "breaks" in the process of executing the program. It may also involve review of the source code of the software using automatic tools to check for common programming errors, and using manual reading to check for functional compliance with our election laws.

In this paper, the term "software" will be used to refer to the computer programs that were used in the Automated Election System (AES) 2010, the first computerized election of May 10, 2010, synchronizing national and local elections. Most of these software were licensed by Smartmatic International from Dominion Voting Systems of Canada, which is the copyright owner of most of these programs. Below is a list of these software, together with their role in AES 2010[3].

(a) Election Management System (EMS) – can be used to design the election, can import data from the Comelec databases, and output data for the EED/EPS and BPT/CCT,
(b) Election Event Designer (EED) – can create ballot designs and configuration data for CF cards and iButtons.
(c) Election Programming Station (EPS) – can be used for mass production of CF cards and iButtons. This program may not have been included in the certification, because it failed to run when tested.

This paper for the EU-CenPEG Project 3030 was prepared by Pablo Manalastas, PhD, IT Consultant for Project 3030; and Lecturer in Computer Science, Ateneo de Manila, Q.C.

(d) Ballot Production Tool (BPT) – originally used by Smartmatic in previous elections to produce the ballot printout for their Direct Reading Electronics (DRE) computers. Can be used to create configuration data on USB-keys for the CCS-REIS canvassing computer. Should therefore be renamed to CCS Configuration Tool (CCT).
(e) Precinct Count Optical Scanner (PCOS) – can scan ballots manually fed by voters, designed for use at the precincts.
(f) Consolidation/Canvassing System – Real Time Election Information System (CCS-REIS) – can do the canvassing at the municipal/city/district/provincial/national levels. This is actually made up of two programs, REIS Listener that reads incoming data from the network, and the REIS Canvasser that actually does the consolidation and canvassing.

Legal Basis of TEC Certification

The Technical Evaluation Committee (TEC) of the Commission on Elections (Comelec) is made up of representatives from the Department of Science and Technology (DOST), the Commission on Information and Communications Technology (CICT), and the Comelec itself. The functions of the TEC in the Automated Election System (AES) 2010 are listed under Section 9(11) of Republic Act 9369[3a], which states that,

"The Committee shall certify, through an established international certification entity to be chosen by the Commission from the recommendations of the Advisory Council, not later than three months before the date of the electoral exercise, categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act based, among others, on the following documented results:

1. *The successful conduct of a field testing process followed by a mock election event in one or more cities/municipalities;*
2. *The successful completion of audit on the accuracy, functionality and security controls of the AES software;*
3. *The successful completion of a source code review;*
4. *A certification that the source code is kept in escrow with the Bangko Sentral ng Pilipinas;*
5. *A certification that the source code reviewed is one and the same as that used by the equipment; and*
6. *The development, provisioning, and operationalization of a continuity plan to cover risks to the AES at all points in the process such that a failure of elections, whether at voting, counting or consolidation, may be avoided.*

Certification by the TEC is not a mandatory requirement of RA-9369, since Section 9(11) gives Comelec a way out of this certification, namely,

"If the Commission decides to proceed with the use of the AES without the Committee's certification, it must submit its reasons in writing, to the Oversight Committee, no less than thirty (30) days prior to the electoral exercise where the AES will be used".

The Oversight Committee mentioned here is the Joint Congressional Oversight Committee (JCOC)[3b] tasked to monitor and evaluate the implementation of RA-9369.

Comelec actually decided to go through with TEC certification, by appointing an international certification entity, SysTest Labs[3c] of Denver, Colorado, in October 2009.

Objectives of this Paper

This paper has the following objectives.

[A] To describe, based on documents obtained from Comelec, the activities done by Comelec and TEC towards *certifying x x x categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of RA-9369* in particular, emphasizing Comelec/TEC activities that carry out the three objectives, *(2) The successful completion of audit on the accuracy, functionality and security controls of the AES software; (3) The successful completion of a source code review; (5) A certification that the source code reviewed is one and the same as that used by the equipment;*
[B] To present this author's personal subjective analysis and critique of these activities.

TEC Certification through SysTest Labs

Comelec announced[3c] the appointment of SysTest Labs on October 8, 2010, "to review and certify the source code of the Automated Election System pursuant to provisions of RA 9369 Sec. 9". Now Section 9 includes provisions on the Comelec Advisory Council (CAC) [Sec 9(8)], the functions of the CAC [Sec 9(9)], the TEC [Sec 9(10)], and the functions of the TEC [Sec 9(11)]. The relevant section is Sec 9(11), which specifies that the TEC shall certify, through SysTest Labs, that the computerized election of 2010 is operating properly, securely, and accurately, and we quote:

"The Committee shall certify, through an established international certification entity x x x categorically stating that the AES x x x is operating properly, securely, and accurately, in accordance with the provisions of this Act (RA-9369)

Section 9(11) is clear on the standards to use to determine proper, secure, and accurate operation of the AES, namely the provisions of RA-9369. If SysTest decides to use another country's standards for its certification, such as the U.S. EAC 2005 VVSG[4], it is duty-bound by conditions of its appointment to check the AES for conformity to RA-9369 first. Any additional checking against another standard should be considered bonus for Comelec.

On March 10, 2010, five months after SysTest's appointment, the TEC submitted to Comelec the document TEC Resolution No. 2010-002[5] in which it *"resolves to certify that the AES, as submitted, with full adoption of the recommended compensating controls*[5a]*, can securely, accurately, and properly be used by voters, boards of election inspectors, local and national board of canvassers, and Comelec in the May 10 National and Local Elections"*.

TEC Resolution 2010-002 has several annexes, including the following [i] a SysTest Labs report entitled, "Certification Test Report Summary for AES May 2010", Revision 1.00, [ii] a SysTest Labs report entitled "Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System" (SCRRST Report), Revision 1.06, dated February 9, 2010, and [iii] a report of the "Source Code Review Team" of the Advanced Science and Technology Institute of the DOST submitted to the TEC, entitled, "Discrepancies Reports Analysis: Final Report", dated February 24, 2010. We describe each of these annexes below.

We note that the wording of the TEC resolution differs from the wording of Section 9(11) which requires the TEC to certify "*categorically stating that the AES x x x is operating properly, securely, and accurately, in accordance with the provisions of this Act (RA-9369)"*. The TEC resolution had to be worded differently from what the law requires, since SysTest (and TEC) found too many test issues that it had to report to Comelec in a Discrepancy Report for resolution or comment. To date, many of these issues are still unresolved. There seems to be no report from Comelec stating whether or not the "compensating controls"[5a] mentioned in the TEC resolution have been put into place. Also we believe that SysTest may not have done a proper source code review and testing, and we have a long list of issues relating to provisions of RA-9369 that SysTest Labs failed to address.

We give details of the SCRRST Report below.

1. SysTest Labs Source Code Review

The Smartmatic Automated Election AES (SAES) for Philippine Election 2010 includes the following election programs: EMS, EED, EPS, BPT-CCT, PCOS, CCS-REIS. It is not clear from the documentation which of these programs are not licensed from Dominion Voting Systems of Canada (Dominion), but it is probable that all of them are from Dominion, except possibly the BPT-CCT. SysTest Labs did manual and automatic source code review of a majority of these programs[6]. The TEC Resolution 2010-002 specifically stated that the programs running on the Comelec public website, KBP server, central server, back-up central server, election system DNS server, PCOS modem firmware, and BPT-CCT were not included in the certification. But the KBP server, central server, and back-up central server are essentially running the same CCS-REIS server program that runs on the municipal BOC, provincial BOC, national Comelec BOC, and national Congress BOC, so the source code review findings for the CCS-REIS server equally applies to these servers.

The programs were written in C#, C/C++, and Java. The SCRRST Report is a bit confusing as to which programming language was used for which program. For example the EMS is supposed to be in C# and the CCS-REIS in Java, but we are told that 1,253 files are shared in common between EMS and CCS-REIS. We hazard to guess that these shared files might actually be in Java, since Java is portable to both Windows computers running EMS, and Ubuntu Linux computers running CCS-REIS.

The SCRRST Report stated as summary that the SysTest Labs review "revealed no evidence of any intentionally written instructions to yield any but the correct results". The report did not state that the election programs are operating properly, securely, and accurately, in accordance with the provisions of RA-9369. The review pointed out many errors in programming, and the severity of these errors may be critical, major, or minor. Here are some of the errors in the source code of the election programs that SysTest pointed out. All these errors are important, and should be resolved, but I have indicated in bold face the errors that I believe are the most important.

1. There is a lack of comments in the Java and C# code.
2. **Many database (DB) transactions are improperly terminated, containing errors in transaction terminating logic, or transactions are explicitly committed even after DB operations' failure. This could cause the CCS-REIS to produce the wrong COC and/or SOV, and the public website to produce incorrect html pages.**
3. There are cases of access to attributes of improperly initialized or uninstantiated objects.
4. There is the problem of maintaining 1,253 identical program files shared by EMS and CCS-REIS, and 32 files that exist in both EMS and CCS-REIS that now have separate maintenance tracks.
5. There are instances of debug code that the programmer used for unit testing that were not removed in the final version.
6. There are logging functions in the CCS-REIS that omit the date and time from the logged messages.
7. The VVSG recommends that all activities and events which require user actions or responses be entered into the logs. This is not always done.
8. The EMS databases can be corrupted due to the possibility of user injection of SQL commands outside of the EMS program.
9. Unencrypted user passwords were stored in the EMS database, creating a big security risk. 10. Encryption keys were hard-coded in the source code of the EMS, making them available to anyone who has access to the executable binary.
11. The EMS code contained narrowing conversions, like conversion of a floating point variable to a narrower integer variable, resulting in loss of precision.
12. The EPS code in C++ contained many instances of memory allocation using "new", without the corresponding de-allocation using "delete", which may result in serious "memory leaks". The report did not use the term "memory leak", but that is now an industry-accepted terminology, so we use it here because of the importance of eliminating memory leaks in proper programming practice.

13. In the PCOS code, several entities may write to a single log file using the function logFile.LogMsg() without clear controls over ownership of the file handle.
14. In the PCOS code, the activities related to connecting to and disconnecting from a wireless device are not logged; for example the identity of the wireless device is not logged.
15. **The PCOS code in C++ contained many instances of memory allocation using "new", without the corresponding de-allocation using "delete", which may result in serious "memory leaks". This could cause the PCOS to hang (stop working) while being used.**
16. In the PCOS code, buffers for holding arrays of text strings are limited in number and each string is limited in size, making it possible for buffer overflow conditions to arise.
17. This item and later items refer to the EMS, CCS-REIS Listener, and CCS-REIS Canvasser source code. The main audit logging function does not include the date and time in the logged message.
18. In Java code, handles should be created in a "try" block and closed in a "finally" block. There are many instances when handles are created but not closed at all.
19. **The CCS-REIS canvasser source code that parses the received EML files were able to extract and record null votes, empty votes, overvotes, and valid votes, but not undervotes. Smartmatic explained that null votes were used to track undervotes. This is obviously wrong – please see explanation in the End Notes[7]. This could have been the reason for the numerous null votes that the Liberal Party complained about.**
20. The Certificates of Canvass and the Statement of Votes are not encrypted before transmission[8].
21. The CCS-REIS code used many deprecated (outdated) methods/functions. Code using deprecated methods should be rewritten to use the new and improved replacement methods/functions.

SysTest stated that the reviewers found *"a wide array of basic programming errors in the Smartmatic source code x x x that give the reader pause to consider the extent of internal quality control measures that the subject (Smartmatic) code may have been subjected to prior to submission to SysTest"*. This assessment from SysTest pointing to *"a wide array of basic programming errors"* is proof that Smartmatic's programs are not fit to use for Election 2010. However, SysTest minimizes the possible effect of these errors in actual usage by stating, after each error is pointed out, that "Given the testing done to date without corruption issues being raised, would indicate that the risk is minimal in a normal path of execution". *Here, SysTest is telling us that even in the presence of these programming errors, Smartmatic's programs may still be used, because SysTest did not encounter any bad effects of these programming errors while they were running the programs using test data. What SysTest is not telling us is that under actual Philippine election conditions, these programs will be exercised/abused to their limits, and probably beyond, because of the sheer magnitude of the numbers involved in our elections. Programming errors that did not manifest when small test data were used will be dramatically revealed with the kind of numbers that we have in AES 2010.* We are talking of 350 candidates' names per ballot, 1600+ distinct ballot designs for 1600+ different local elections, 1000 voters per PCOS, 51 million voters in 76,000 precincts, etc. In the places where these Smartmatic's programs were previously used, namely in the U.S., there were only two candidates and not as many voters. To prove our point that the election programs can malfunction because of the programming errors pointed out by SysTest, we see in Comelec's election results website concrete evidence of programs that have *actually* malfunctioned, evidence such as, HTML pages with no results for certain positions when there are results for others, or HTML pages that are improperly formed such as a <td> tag without a corresponding </td> closing tag, and so on.

Despite the serious danger of malfunction because of the wide array of programming errors, the TEC and Comelec were only too glad to accept that the Smartmatic programs "*can securely, accurately, and properly be used by voters, boards of election inspectors, local and national board of canvassers, and Comelec in the May 10 National and Local Elections".*

We require college students to program in many of the computer courses that we teach at the Ateneo de Manila[9]. If our students submit code that is full of bugs, like the Smartmatic election programs, then we return the code to our students, so that they can rewrite them, and resubmit them when they are reasonably bug-free. This is what Comelec should have done -- return the code to Smartmatic to rewrite until the code is reasonably bug-free, and in the meantime, Smartmatic should refund a reasonable amount to Comelec, as compensation for the trouble and time spent in trying out Smartmatic's buggy programs.

Note that SysTest Labs only checked for generally desirable program features like proper initialization of variables, proper allocation and deallocation of memory, properly terminated database transactions, and other similar desirable programming practices. Except for the mention of improper audit logging, there is no indication that SysTest checked for desirable features of election programs in general, nor was there any mention of conformity of Smartmatic's programs with RA-9369 and Comelec TOR in particular. Nowhere in the Source Code Review section of the SCRRST Report did SysTest Labs mention that it checked for conformity of the Smartmatic election programs to important provisions of RA-9369 and the Comelec TOR -- program features that are so important that these have become the subject of intense debate in the media and on the Internet between Comelec and election watchgroups. After all, Comelec paid SysTest Labs PHP70 million[10] to certify, *"categorically stating that the AES x x x is operating properly, securely, and accurately, in accordance with the provisions of this Act (RA-9369)"*

The questions that we would like SysTest Lab's source code review to have answered are given later in this paper.

2. SysTest Labs Readiness Testing & Security Testing

Testing is done by running the executable programs (the source code is not needed during testing) on computers that are exactly the same as those that will be used during elections, using test data supplied by Comelec, and using test suites (test methods) that the testing company considers appropriate. The Wikipedia[11] states that "a primary purpose of testing is to detect software failures so that defects may be discovered and corrected x x x Testing cannot establish that a product functions properly under all conditions but can only establish that it does not function properly under specific conditions (using the given test data) x x x software testing includes execution of that code in various environments and conditions as well as examining the aspects of code: does it do what it is supposed to do and do what it needs to do x x x Functional testing refers to tests that verify a specific action or function of the code x x x Functional tests tend to answer the question of 'can the user do this' or 'does this particular feature work' "

[a] Readiness Testing.

SysTest Labs readiness testing "is designed to validate that the core functionality of the voting system is intact and functioning in a manner consistent for the expected implementation"[12]. The readiness test covered the EMS, EED, PCOS, and CCS-REIS. Below, we give the results of the readiness testing done by SysTest, to give the reader an idea of the scope of functions of each of the programs mentioned[13].

For the EMS, "the user was able to log in, create jurisdictions, voting locations, candidates, offices, parties, etc., implement the data import tool as well as all other basic data entries that go into an election definition. The EMS was able to output the expected CCS configuration files and data files for the EED"

"The EED was able to import data from the EMS, create ballot content and styles, including the definition of individual contest layouts (ballots?). The EED was also able to create election definition files as well as move them to the associated compact flash card. iButtons were also able to be created through the EED."

For the PCOS, "The machine was able to be booted and logged in to. Polling counts validated to be zero, polls opened and ballots cast. The polls were closed and reports tallied". Transmission was not tested, since the proper environment was not available.

For the CCS, "The system did not allow entry, until a work-around was introduced that x x x turned off a token validation that regulates entry" into the CCS. "Once the CCS was able to be accessed (by turning off a token validation), data (election returns?) was imported and tallies and reports generated".

We believe that the readiness tests conducted by SysTest Labs on the AES 2010 computers, while validating "that the core functionality of the voting system is intact", could not have validated that the core of the voting system is

"functioning in a manner consistent" for Philippine elections. This is because the readiness tests are superficial and used insufficient data artificially contrived by Comelec, and did not have any bearing at all on the real data of Philippine elections. We have more to say about this in a later section on what the readiness test did not cover.

[b] SysTest Labs Security Testing.

SysTest Labs conducted three sets of security tests on the EMS, EED, PCOS, and CCS-REIS[14].

[i] The *Physical Access Measures* test suite is designed to test the policies, measures, and procedures developed by the vendor (Smartmatic) to physically secure the voting equipment in both a public and private environment x x x This test also validates that the vendor has developed and documented procedures to enable poll workers to physically protect and perform an orderly shutdown of the voting system, protect the system during repair or maintenance and maintain physical security at central count stations. Functionality and placement testing is also performed on the PCOS taking into account location of locks, seals, and tamperproof devices.

[ii] The *Access Control* test suite is designed to test the policies, measures, privileges and procedures developed by the vendor to control access to the voting equipment and their interfaces in both public and private environments. For the PCOS, this test suite checks for the access to audit logs and counters without proper authentication and voter access to functions during voting mode.

[iii] The *Software/Firmware Security* suite tests documentation of software distribution, documentation and comparison of the software validation, the protection against malicious software, the software and firmware installation, data and document retention, the protection from (of) improper data entry and/or retrieval. Additionally, the test suite ensures the voting can provide system functions that are executable only in the intended manner and order, and only under the intended conditions, use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met, and has a means to implement a process for restricting and/or controlling access to a system function.

The following results of the Physical Access Measures tests were reported by SysTest Labs. For the EMS, EED, PCOS, and CCS, there is no proper documentation for mandatory administrative procedures or an adequate recommendation for a general hardware access controls policy. Measures are not provided to protect against tampering during maintenance activities. The documentation may (EMS, PCOS) or may not (EED, CCS) provide procedures for safeguarding the audit logs. The PCOS does have a procedure for shutting down, but not one to counteract an emergency situation that includes closing the polls (shutting down) and securing the voting equipment.

The following results of Access Control testing were reported by SysTest Labs. Typical would be the report on the CCS. "The documentation does not provide components of a general access control policy for software access controls, communications, effective password management, protection abilities of a particular operating system, general characteristics of supervisory access privileges, segregation of duties, and any additional relevant characteristics. The documentation does not describe access control measures for program unit ownership and other regional boundaries, one-end or two-end port protection devices, security kernels, computer-generated password keys, special protocols, message encryption, controlled access security and methods used to prevent unauthorized access to the access control capabilities of the system itself x x x". Although this report appears to be in English, I believe there is a better and clearer way of writing it.

The following results of Software/Firmware testing were reported by SysTest Labs. Typical would be the report on the CCS. "The documentation does not include software distribution, comparison of the software for validation, how to protect against malicious software, and the software firmware installation locations. Data and document retention was documented, the voting system protects against improper data entry or retrieval. The voting system can provide system functions that are executable only in the intended manner

and order, and only under the intended conditions and use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met. But does not incorporate a means of implementing a capability if access to a system function is to be restricted or controlled". Again, this report appears to be in English, but I believe that there is a better and clearer way of writing it, considering the P70 million that Comelec paid SysTest Labs.

To summarize, despite all the many serious programming errors discovered by the SysTest Labs source code review, and despite the many negative findings discovered by the security tests, SysTest Labs concluded in favor of the AES, saying, "Taking all current findings into consideration, as well as the tests completed to date, SysTest Labs does not find reason to preclude the AES voting system as being suitable for use as an electronic election system for the Republic of the Philippines". Why did SysTest Labs not specifically mention the Smartmatic AES voting system? Is it because Smartmatic AES did not, and could not, pass the standards for election systems set by SysTest Labs?

3. TEC's Discrepancies Reports Analysis

The Discrepancies Reports Analysis[15] was prepared by the Source Code Review Team (SCRT) of the Advanced Science and Technology Institute (ASTI), upon the request of the TEC to aid it in its work of certifying the AES 2010. SysTest Labs submitted to Comelec a list of discrepancies that were still open and unresolved, and it is this list that ASTI-SCRT used as a basis for its analysis.

[a] On the issue of undervotes and overvotes.

The ASTI-SCRT report mentioned that "it was understood in the discussion with Alejandro Garcia (Heider Garcia?) that Smartmatic used the term "nullVote" for "under vote" and "emptyVote" for "over vote". Daniel Mora of Smartmatic corrected this impression, and said that "Smartmatic was actually using the variable "nullVote" for "over vote" and "emptyVote" for "under vote". The ASTI-SCRT suggested that Comelec clarify the definitions and determine whether or not to accept Smartmatic's use of nullVote and emptyVote.

Daniel Mora's version of the definitions, though reasonable, is not adequate to capture the facts of Philippine elections. As a mathematician-turned-computer-programmer, I strongly suggest the following "better" definitions[7].

The variable "*nullVote*" should be used for votes that cannot be counted as valid votes and must be nullified, as in the cases of inadequate shading and overvotes. If the voter's mark in the oval is below the threshold, the PCOS cannot decide whether the mark is a vote or not, and so nullifies the vote instead. A vote is an *overvote* if in a candidate position (contest) with N choices, the voter chose more than N, and so the PCOS will not know to whom to give the N votes, and so nullifies all the voter's choices instead. Thus inadequate shading and overvotes should be counted as nullVotes.

A vote is an *emptyVote* if, for a given candidate position (contest) the voter did not make any choice/mark on any candidate's oval -- it is considered to be equivalent to "none of the above", and so it is a valid vote meaning "abstain".

A vote is an *undervote* if in a candidate position (contest) with N choices, the voter chose less than N, and in this case the PCOS will consider all the votes as valid votes.

A vote is an *exact vote* if in a candidate position (contest) with N choices, the voter chose exactly N candidates, and so each one of his choices is a valid vote.

Thus the *valid votes* are empty vote, undervote, and exact vote, and the *invalid votes* are the null votes, meaning inadequate shading and overvote.

So Alejandro Garcia's opinion to use null votes to track undervotes is wrong, because null votes are not included in the count, while undervotes in which there is at least one vote is included in the count. Furthermore, Daniel Mora's opinion to use emptyVote for under vote is also wrong, since emptyVote is not included in the count, but under vote is included in the count.

[b] On the issue of errors in database transaction handling.

The SysTest Labs report mentions many database transactions that are improperly terminated, or contain errors in transaction terminating logic, or transactions are explicitly committed even after database operation's failure. This could cause the CCS to produce the wrong COC and/or SOV, and the public website to produce incorrect html pages. The ASTI-SCRT report does not even mention this issue.

[c] On the issue of memory allocation errors in the PCOS.

The SysTest Labs report mentions that the PCOS code in C++ contained many instances of memory allocation using "new", without the corresponding de-allocation using "delete", which may result in serious "memory leaks". The PCOS, with only 512MB of memory, which is used for both ram and ramdisk, could hang (stop working) while being used on election day, due to memory leaks. The ASTI-SCRT report does not even mention this issue.

What's Wrong With TEC Certification?

The function of the TEC is given in Section 9(11) of RA-9369:

"The Committee shall certify, through an established international certification entity to be chosen by the Commission x x x categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act x x x"

The problems with Comelec/TEC using an international certification agency like SysTest Labs are many. First Comelec does not know exactly what constitutes certification, and neither the CAC nor the TEC were of much help in this regard. And so SysTest was more-or-less allowed to do its "thing". Second, SysTest Labs, being an international certification entity, is used to certifying for conformity to U.S. EAC 2005 VVSG, and so certified the Smartmatic AES with respect to this standard, and completely forgot conformity of the Smartmatic AES to Philippine election laws. Third, SysTest Labs, in our personal opinion, was so lenient in its evaluation of Smartmatic, with which it had previous favorable engagements, that it was willing to forget the many serious programming errors and inadequacies in security of the Smartmatic AES. Fourth, the TEC should have gone beyond the work submitted by SysTest Labs, and insisted that SysTest Labs test for conformity to RA-9369 and the Comelec TOR, first and foremost.

Important Questions that SysTest Labs' Source Code Review Did Not Address

Among the questions that we would like SysTest's source code review to answer, but SysTest Labs did not even address are the following.

1. Data preparation and data conversion are initially the most tedious and time-consuming activities of the election computerization exercise. Are there automatic conversion tools that were provided by Smartmatic to Comelec to convert data in the Comelec databases into the form acceptable to the EMS program, or was a substantial work done manually? How much handholding did Smartmatic do? Can Comelec do this for the next election without help from Smartmatic? Was the conversion program checked for correctness, by making it part of the source code review?

2. Can the data structures of the EMS program be made large enough to hold data for each of more than 1600 ballot designs, each ballot containing 266 candidates' names[28] on one side and less than that number on the other side? In the previous electoral exercises elsewhere in the world that used paper ballots with voting machines, the figures were much smaller than this.

3. Can the EMS program be conveniently used to design an election where the congressional seat allocation can vary from jurisdiction to jurisdiction? For example, there are cities containing one or more congressional districts, and there are congressional districts containing one or more cities and municipalities[29]. Is the EMS program flexible enough to handle such variations in hierarchical organization?

4. Do the functions/procedures to read/write EML data[30] follow the published EML standards, so that EML data (precinct ER) written by the PCOS program can be properly read by the municipal CCS-REIS, the EML data (COC) written by the municipal CCS-REIS can be properly read by the provincial CCS-REIS, etc.?

5. For each of the more than 1,600 ballot designs, are the row-column coordinates of each of the 266 candidates names-and-ovals on each of the two faces of the ballot faithfully written on the CF-card that will be used to configure the PCOS program for the precinct? The faithful writing of the correct coordinates will ensure that a vote mark for a candidate will be credited to that candidate by the PCOS program. Furthermore, suppose that candidates' details for ballot design no. 1437 have been written to CF card no. 1437, is there a provision in the PCOS program that uses CF card 1437 to accept only ballots with design no. 1437? With such a provision, then the ballot-face-to-CF-card problem[31] that occurred on May 3, 2010 can be avoided.

6. Does the PCOS program employ both area-computation algorithm and boundary-recognition algorithm so that it can accept the following marking styles that the voter is allowed to use to mark his ballot: full shade, partial shade of majority of the oval, cross mark, check mark, distinct single dot at the center of the oval? These marking styles are allowed by the Comelec TOR, but Comelec finally decided to allow only full shade and partial shade of majority of the oval, probably because of limitations in the mark recognition algorithm used by the PCOS program.

7. Does the PCOS program contain functions/procedures that will allow the voter to verify (visually at least) how it read and interpreted his ballot, by showing the voter a list of the candidates that it thinks he voted for? This feature will serve as a check of the mark-reading accuracy of the PCOS program and also serve as a check of the faithfulness of the copying of the row-column coordinates of the candidates from the ballot face to the CF-card, which we listed in Question 4. Also this is in conformity with the provision of Section 7(n) of RA-9369[32]. Furthermore, we must ask the question, is this feature a permanent part of the PCOS program that the Comelec cannot disable?

8. Is there a function/procedure in the PCOS program and in the CCS-REIS canvassing program that will allow the BEI/BOC/OfficialWatcher/KBP-Rep/PPCRV-rep to verify at any time during voting/canvassing that the program running on the PCOS/REIS is one and the same as the program that was certified by the TEC, in conformity with the provision of Section 11, Item 5[33], of RA-9369?

9. Do the logging functions of the PCOS provide enough detail in the audit logs that indicate the state of appreciation of each voter's mark on the ballot, whether overvote or undervote, or no vote, or mark is below the threshold allowed as vote mark -- so that the PCOS can recommend manual appreciation of the ballot in one or more of these cases (say, mark is below the threshold), and so that such cases can be used as a basis of an electoral protest and such ballots can be used for the ensuing recount[34]?

10. Do the logging functions of the PCOS state the reason for rejection of a ballot, and will the program segregate the rejected ballots in another bin, so that such rejected ballots can be used as a basis of an electoral protest, in case the PCOS made an error in classifying the ballot as rejected? Under normal conditions, if the ballot was given by the legal BEI to the legal voter, no ballot should be rejected by the PCOS -- and under such conditions, rejection of the ballot indicates PCOS error.

11. Is there a function/procedure in both the PCOS program and the CCS-REIS program that can specify that a particular run is either (1) testing run, or (2) actual election run, so that a CCS-REIS program on an actual election run will not accept results from a PCOS that is on a testing run? With this feature, the inclusion of FTS results in the actual canvassing could have been avoided[35].

12. Is there a feature of the ballot, the PCOS program, the CCS-REIS program, and the Public website, that will allow each individual voter to check from the public website that all of his votes were included in the canvassed count, without revealing the identity of the voter? One way to do this is to assign a unique random number to each ballot, and to assign a unique random number to each candidate on the ballot. The random number of a candidate will vary from ballot to ballot. While a voter is filling out his ballot, he needs to copy his ballot random number, and the random number of each candidate that he voted for. At the end of the canvassing period, the voter can visit the Public Website, and enter his random ballot number, and the Website will tell him which of his candidate's random numbers were included in the count[36].

13. Does the PCOS program implement digital signing of the precinct ER before transmission? Is OpenSSL[37] API used for digital signing, or else a similar open standard used? Is the public key of the signer included with the signature? Is the public key certified by a Certificate Authority that is included in the list of recognized CAs? Is the signer a BEI included in the list of authorized BEIs for the precinct? Is a similar digital signing feature available on the CCS-REIS program at all levels of canvassing? Digital signatures on the election documents (ER, COC, etc) are required by RA-9369.[38]

14. Does the digital signing procedure compromise the private key of the signer? The private key is compromised if the PCOS/CCS-REIS is able to read the private key of the signer from the medium (USB key, CD, DVD) presented by the signer, since only the signer should be able to read/know his private key. In case the private key is compromised, the owner of the private has to request his CA to revoke his signing keys, thereby rendering his private/public keys useless for signing purposes.

    A solution to the problem of signing the ER/COC without revealing the signer's private key is to use a processor SmartCard[39] (computer-on-a-card) for digital signing. From the precinct ER, the PCOS computes a message digest M, then the PCOS tells the signer to insert his SmartCard into the SmartCard reader of the PCOS. The PCOS then gives the SmartCard the message digest M, and the computer-on-the-SmartCard encrypts M with the private key P of the signer, to produce the digital signature D. The SmartCard then gives this value D to the PCOS, completing the digital signing process without telling the PCOS the value of the private key P of the signer. Neat!

    Since the Dominion-Smartmatic PCOS used during Election 2010 did not have a SmartCard socket, it could not have done digital signing in the manner described in these paragraphs, which, by the way, is one of the few legal ways to do this (lawyers please take note!)

15. The reviewers of the Dominion-Smartmatic source code from SysTest Labs pointed out numerous cases of errors in database operations[40], resulting in the corruption of canvassing tables. How many of these errors in database operations still remain in the Dominion-Smartmatic source code? Could the following truly glaring error be the result of these errors in database operations? -- the Public Website lists 21,766 clustered precincts in which one or more candidate positions do not have any entries, namely, there are no candidates' names and no number of votes. The title for the candidate position is not even there, and in its place, the word “$contestResult” appears[41]. Now 21,766 precincts out of a total of 76,000 precincts is a whopping 28.6%. With a percentage error of 28.6% of precincts, can you believe that Smartmatic-Comelec did the canvassing correctly?

Important Questions that SysTest Labs' Testing Did Not Address

For the readiness and security tests, SysTest Labs used test data provided by Comelec, and these data are artificially contrived "toy" data, since actual "hard" election data were not yet available in October 2009.

Thus SysTest Labs could not test if the EMS is the appropriate tool for designing the more than 1,600 local election contests, in which each contest had about 350 candidates, which will involve 51 million voters who will vote in more than 76,000 clustered precincts. The EMS has never been used to manage election design at such grand scale before, ever!

Also SysTest Labs could not test if the data on more than 1,600 ballot face designs produced by the EED were correctly configured into the CF cards for use by the more than 1,600 differently-configured PCOS computers. Testing that the 1,600 ballot faces are correctly captured as CF-card data for the PCOS is probably the single most important activity in SysTest Labs' test suite, since this plays a vital role in the correctness of the election count, and *SYSTEST LABS DID NOT DO THIS TEST*.

Instead Comelec gave the BEI teachers instructions to use ten test ballots to test that votes for the each of the 350 candidates in their specific local (and national) elections are correctly credited to the proper candidate. This test activity assigned to the teachers is both mathematically and statistically impossible, since for Party List alone, you need more than 180 test ballots to check that a vote for each of the more than 180 Party Lists will go to the correct party list. The question that begs to be asked is: Why did Comelec give to the teachers the job of ascertaining correct counting functionality to the BEI teachers, who are not testing professionals, when that is the job of SysTest Labs!

Implications of Improper TEC Certification on Election Day

This report has made clear in its many pages that certifying an AES that is not appropriate for Philippine Election 2010 can have many disastrous effects on the correctness of the count, and has put the result of this election, in the mind of computer programmers if not in the consciousness of Comelec, in serious doubt. This is the same as saying that there was a failure of computerized election count, if not a failure of election.

Best Industry Certification Practice

Certification is the practice before closed-source commercial software is deployed, so that the country's election agency can have reasonable expectation that the programs will work properly. But certification is not needed, but only recommended, when the country's election law provides for source code review by third parties independently of the election agency.

Thus, more and more states in the U.S., and more and more countries who are computerizing their elections, are turning to public source code review to verify the correctness of their country's election programs.

Analysis and Conclusion

The Technical Evaluation Committee (TEC) of the Comelec certified on March 9, 2010, that the AES, as submitted by Smartmatic, and as reviewed and tested by SysTest Labs, with full adoption of about 30 groups of compensating controls, can securely, accurately, and properly be used by voters, boards of election inspectors, local and national boards of canvassers, and the Comelec in the May 10, 2010 National and Local Elections.

The certification function of the TEC is contained in Section 9(11) of RA-9369, and we quote, *"The Committee shall certify, through an established international certification entity to be chosen by the Commission x x x categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act x x x"* The TEC could not certify that *the AES is operating x x x in accordance with the provisions of this Act (RA-9369)* since SysTest Labs did not check the AES

for conformity with RA-9369, the Comelec TOR, and implementing regulations, but checked the AES for conformity only with certain provisions of the U.S. EAC 2005 VVSG.

Furthermore, SysTest Labs' source code review found many instances of serious programming errors in Smartmatic's programs that may cause, and actually did cause, execution errors on election day, as evidenced by the PCOS program malfunctioning, the PCOS and CCS allowing transmission of FTS results, and a significant number of tabulation errors in the Comelec's public website. Also, SysTest Labs did not test the election design produced by the EMS and the EED for the actual May 10. 2010 election, but only tested the artificially contrived "toy" data supplied by Comelec. Thus there is no way that SysTest Labs could certify that the AES is operating properly, securely, and accurately in accordance with the provisions of RA-9369 because it did not test the AES as it will be used on election day.

To conclude, although the TEC and SysTest certifications revealed serious errors in the source code of the AES, and inadequate security provisions of the AES, such observations could have been arrived at for much less than the PHP70 million that Comelec spent for certification, which was optional anyway.

End Notes:

[1] The definition of "certification" is given here, http://www.astqb.org/educational-resources/glossary.php

[2] The definition of "software testing" is given in the article, http://en.wikipedia.org/wiki/Software_testing

[3] The report entitled, "Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System", dated February 9, 2010, describes the list of software included in the review done by SysTest Labs in the section "3 System Overview" on pages 5-7, and in the section "Readiness Testing Overview" on pages 28-29.

[3a] Republic Act 9369 is available from http://www.chanrobles.com/republicactno9369.html.

[3b] Section 27 (33) of RA-9369 gives the composition and functions of the JCOC.

[3c] The appointment of SysTest Labs, Inc (SLI) is given in this news article, http://www.comelec.gov.ph/modernization/2010_natl_local/press_releases/COMELEC_awards_source_code_review_to_US_based_SysTest_Labs.html

[4] This is the United States Election Assistance Commission (EAC) 2005 Voluntary Voting System Guidelines (VVSG). The guidelines are downloadable from the webpage, http://www.eac.gov/testing_and_certification/2005_vvsg.aspx

[5] TEC Resolution No. 2010-002 is entitled, "Certification of Automated Election System (AES) for the May 10, 2010 National and Local Elections". The resolution was signed by Denis F. Villorente (ASTI/DOST), TEC Chairman, Ester L. Villaflor-Roxas (Comelec), TEC Member, and Angelo Timoteo M. DIaz de Rivera (NCC/CICT), TEC Member.

[5a] These compensating controls are listed in the document entitled, "Technical Evaluation Committee: Compensating Controls on the AES for the May 10, 2010 National and Local Elections", a 30-page document that lists thirty (30) groups of compensating controls.

[6] The SysTest Labs report entitled, "Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System", dated February 9, 2010, describes the source code review done by SysTest Labs in "4 Source Code Review" on pages 8-27.

[7] I could not find a universally accepted definition of the terms null vote, empty vote, overvote, and undervote, so being a mathematician-computer-programmer, I decided to adopt the following definitions, which are the most mathematically reasonable in the context of elections using voter marked paper ballots that are fed to PCOS election computers. A vote is a *null vote* if the voter's mark in the oval is below the threshold, and so the PCOS can not decide whether the mark is a vote or not, and so nullifies the vote instead. A vote is an *empty vote* if the voter did not make any choice/mark on any candidate's oval -- it is considered to be equivalent to "none of the above", and so it is a valid vote meaning "abstain". A vote is an *overvote* if in a candidate position (contest) with N choices, the voter chose more than N, and so the PCOS, will not know to whom to give the N votes, and so nullifies all the voter's choices; thus an overvote is also a null vote. A vote is an *undervote* if in a candidate position (contest) with N choices, the voter chose less than N, and in this case the PCOS will consider all the votes as valid votes. If the undervote chose zero candidates, then the undervote is also an empty vote. A vote is an *exact vote* if in a candidate position (contest) with N choices, the voter chose exactly N candidates, and so each one of his choices is a valid vote. Thus the *valid votes* are empty vote, undervote, and exact vote, and the *invalid votes* are null vote and overvote. So Smartmatic's decision to use null votes to track undervotes is wrong, because null votes are not included in the count, while undervotes in which there is at least one vote is included in the count.

[8] SysTest claims that the COC and SOV are not encrypted before transmission. However, examination of the MBOC CCS-REIS print logs for a typical municipality like Caibiran in the province of Biliran in Region VIII shows the CCS uploading tallies to https://central.server.rp2010.net/, and the https protocol implies that the MBOC CCS-REIS client has negotiated with the Central CCS-REIS server via the TLS protocol a session key to use for encryption. The https protocol makes possible uploads of encrypted tallies. The TLS protocol is described in the Wikipedia entry on Transport Layer Security, http://en.wikipedia.org/wiki/Transport_Layer_Security. However, SysTest did not see evidence of the use of encryption in the CCS source code, and so the log entry specifying use of the https protocol might actually be an unencrypted transmission of plaintext documents.

[9] The Department of Information Systems and Computer Science (DISCS) of Ateneo de Manila is under the School of Science and Engineering (SOSE). The website of DISCS is http://sose.ateneo.edu/module.php?LM=departments.detail&id=1204865701476. The faculty roster can be found in http://sose.ateneo.edu/system.php?LS=staticpages&id=1205225910750. The personal website of the author is http://curry.ateneo.net/~ambo/

[10] This Inquirer news article mentions Comelec as contracting SysTest Labs for P70 million to do certification of AES2010, http://newsinfo.inquirer.net/breakingnews/infotech/view/20091010-229354/US-firm-to-test-poll-automation-system

[11] The purpose of software testing is given in the Wikipedia article, http://en.wikipedia.org/wiki/Software_testing

[12] The SysTest Labs report entitled, "Certification Test Report for Source Code Review, Readiness and Security Testing: Philippine AES Voting System", dated February 9, 2010, describes the readiness testing that it did on pages 28-29.

[13] The results of readiness testing are from page 28 of the SCRRST Report mentioned in [12]

[14] The security tests are described on pages 30-35 of the SCRRST Report mentioned in [12]

[15] The document, "Discrepancies Reports Analysis: Final Report" is written by the Source Code Review Team (SCRT) of the Advanced Science and Technology Institute (ASTI) and submitted to the Technical Evaluation Committee (TEC), on February 24, 2010.

[28] The ballot used for Philippine Election 2010 for non-ARMM regions contained 266 candidates' names on the front page. See http://www.comelec.gov.ph/downloadables/2010official%20ballot%20asof-0208/national_nonARMM.pdf

[29] For example, the City of Manila has 14 congressional districts: BINONDO, ERMITA, INTRAMUROS, MALATE, PACO, PANDACAN, PORT AREA, QUIAPO, SAMPALOC, SAN MIGUEL, SAN NICOLAS, SANTA ANA, SANTA CRUZ, and TONDO. On the other hand, the first congresional district of the province of Leyte has one city and seven towns: Tacloban City , Tolosa , Tanauan , Santa Fe , San Miguel , Palo , Babatngon , and Alangalang

[30] The standards for the Election Mark-Up Language (EML) are documented in the following places: http://docs.oasis-open.org/election/eml/v5.0/os/EML-Process-Data-Requirements-v5.0.html, http://docs.oasis-open.org/election/eml/v5.0/os/EML-Schema-Descriptions-v5.0.html, http://docs.oasis-open.org/election/eml/v5.0/os/EML-Data-Dictionary-v5.0.html, and http://docs.oasis-open.org/election/eml/v5.0/os/EML-Schemas-v5.0/

[31] This ABS-CBN news article, and subsequent articles, describes the error caused by the mismatch between row-column positions of candidates on the ballot, and row-column positions of candidates contained in the CF card configuration data: http://www.abs-cbnnews.com/nation/05/03/10/errors-force-comelec-reset-pcos-testing

[32] Section 7 of RA-9369 reads as follows: "Minimum System Capabilities. The automated election system must at least have the following functional capabilities: . . . (n) Provide the voter a system of verification to find out whether or not the machine has registered his choice"

[33] Section 11 Item 5 states "Sec. 11. Functions of the Technical Evaluation Committee. - The Committee shall certify . . . categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately, in accordance with the provisions of this Act based, among others, on the following documented results: . . .5. A certification that the source code reviewed is one and the same as that used by the equipment". The sure way to check that the software is "one and the same" is to check the software running on the PCOS and CCS computers, anytime on election day itself.

[34] The electoral protest of Vice Presidential candidate Mar Roxas is reported here, http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20100724-282841/Mar-Roxas-protest

[35] The more than 200 cases of FTS results being included in the canvasses are listed here, http://pmana.multiply.com/journal/item/177/Congressional_Canvass_in_Quandary_Jun_03_10, and those FTS results reached all the way up to the national Congressional canvass,

[36] The following article describes the Scantegrity II system, in which the random numbers are revealed to the voter using a special ink for marking his choices on the ballot: http://www.usenix.org/event/evt08/tech/full_papers/chaum/chaum_html/ScantegrityII.html

[37] The OpenSSL toolkit is described in the website http://www.openssl.org/docs/. In particular, the API is given in http://www.openssl.org/docs/ssl/ssl.html

[38] Section 19 (22) of RA-9369 second to the last paragraph, states, "The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate."

[39] Java processor SmartCards are described in this article: http://www.javaworld.com/jw-12-1997/jw-12-javadev.html

[40] The report is entitled "Certification Test Report for Source Code Review, Readiness and Security Testing", by SysTest Labs, dated February 9, 2010. The errors in database operations (errors in database "commits"), are described in the section entitled "Database Transactions" on pages 14-16.

[41] For example, check out the webpage of a clustered precinct in Antipolo City, namely: http://www.comelec.gov.ph/results/2010_natl_local/res_reg5802271.html . You will see that the three positions: Party List, Vice Governor, and Sangguniang Panlalawigan, do not have any entries, and in place of the entries, the word "$contestResult" appears.