
This paper explains the significance of the issues raised in the report of SysTest Labs Inc. (henceforth called SysTest) dated Feb. 9, 2010 and entitled “Certification Test Report for Source Code Review, Readiness and Security Testing Rev. 1.06” (henceforth called the Report). The Report is essential because it is required by the following provision of the Automated Election System (AES) Law, R.A. 9369:

“SEC. 11. Functions of the Technical Evaluation Committee. – 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 exercises, 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; ...”

We raise the following significant concerns in connection with the Report:

1. **ONE MISSING AND FOUR ABNORMALLY APPENDED PAGES.** The copy of the Report released by the Comelec appears to have a missing page (32 of 32) as well as appended pages of doubtful origin (“33 of 33”, “34 of 34”, “35 of 35”, and “36 of 36”). It is suggested that the Comelec release page 32 immediately and to clarify the authenticity of the abnormally appended pp. 33-36.

2. **MAKE PUBLIC THE DISCREPANCY ANALYSIS BY IFES CONSULTANT.** Attached as Annex C to the Report was a “Discrepancy Report Analysis: Final Report” by the Source Code Review Team of the Advanced Science and Technology Institute of the Department of Science and Technology, dated Feb. 24, 2010. The conclusion of this DOST report says:

   “Considering the results of all the tests conducted by Systest and COMELEC, the analysis by
Michael Yard of IFES on the same discrepancy reports, and the review and analysis conducted by the [DOST] Team, we find no reason to preclude the use of AES in the coming elections in May 2010.” (Summary, last page [no pagination in the original])”

Again, in the interest of transparency, we ask the COMELEC to release to the public the analysis by the IFES consultant, which partly became a basis for the ASTI-DOST team to issue a guarded endorsement of the AES.

3. THE SMARTMATIC SOFTWARE NOW IN USE CONTAINS UNRESOLVED ISSUES. It is presumed that the software reviewed in the Report is the same software in escrow at the Bangko Sentral ng Pilipinas. Thus, whatever shortcomings, problems, and deviations from standards described in the Report which have not been “closed” (i.e., resolved) must still be part of the system deployed for the May 10 elections. Otherwise, if the software has since been modified, then the modified software would be different from what was reviewed in the Report and escrowed at the BSP, which would make the modifications unauthorized and therefore illegal.


“The criteria against which the source code was compared are a sub-set of those as described in the 2005 Voluntary Voting System Guidelines as published by the Election Assistance Commission of the United States.” (Report, p.11)

It is suggested that the Comelec clarify why only a sub-set instead of the full set of the VVSG standards were used and why other portions of the full set of standards were excluded. It is also noted that the 2005 VVSG has been superseded by the updated 2007 VVSG. It is suggested that the COMELEC explain why it accepted outdated 2005 standards when updated 2007 standards were already available.

5. INCOMPLETE AND IRREGULAR DELIVERIES OF SOURCE CODE. The SysTest source code review was conducted Oct. 26, 2009 - Feb. 9, 2010. Smartmatic's submission delays and other problems in submitting their source code for review suggest that the full Smartmatic AES software suite was not ready when the code review started in Oct. 2009. Therefore, the full suite was not ready either in May 2009 when it submitted its bid, or in July 2009, when it signed the AES contract with the COMELEC. Here's how the Report described the:

“Our source code review process typically includes reviewing the entirety of the delivered source code one time, and then using automated source code comparison tool applications to determine, and display for review, the changes in subsequent code submissions. The Smartmatic source code was not delivered in comprehensive submissions on a timely schedule. Dates on which source code submissions were expected were routinely missed, and the code collections that were submitted for review were inconsistent in their content. It was not until December 28, 2009, two months into the project, that the vendor made a singular complete delivery of all of the EMS, Listener and REIS source code.” (Report, p.26)
6. VIOLATION OF LAW: THE SMARTMATIC SOFTWARE HAS NOT BEEN SUCCESSFULLY USED HERE OR ABROAD. It is clear from the Report narrative that Smartmatic was rewriting the AES software during the period when SysTest conducted its review, to make the software comply with VVSG standards.

“After a review of the changes within the newly received versions of files was completed, new, updated discrepancy reports were created and submitted to COMELEC for communication to the vendor. In this iterative fashion, the vendor brought all of those cited findings classified as having the potential for either “critical” or “major” impacts on the voting system into compliance with the VVSG requirements”. (Report, p.12)

This means that the software that came out of the SysTest review and put in escrow at the Bangko Sentral ng Pilipinas has never been successfully used and tested here or abroad, violating the following provision of the AES Law (R.A. 9369):

“Sec. 12. ... With respect to the May 10, 2010 election and succeeding electoral exercises, the system procured must have demonstrated capability and been successfully used in a prior electoral exercise here or abroad. Participation in the 2007 pilot exercise shall not be conclusive of the system’s fitness.”

It seems irregular that SysTest was not only doing a review for the COMELEC, but was also helping the vendor in software development, particularly in making their software conform to VVSG standards.

7. UNRESOLVED ISSUES REMAINING: 5,466. The Report identified a total of 4,422 “critical” or “major” deviations from the 2005 VVSG standards. All of these, according to the Report, have been brought by the vendor into compliance and therefore “closed”. However, the Report also cited 4,897 “minor” deviations from the 2005 VVSG standards which have remained “open” (Report, p.18). Presumably, these remain non-compliant with the VVSG standards. SysTest also identified 569 additional non-standards-related issues, 327 of them “major” and 242 “minor”, that remained unresolved (“open”). Referring to these 569 unresolved issues, the Report says:

“The vendor has of this writing not responded to the findings raised by SysTest as a result of its automated and logical analysis.” (Report, p.27)

Because the SysTest analysis was “static”, “the exact performance of the programs derived from the reviewed source code cannot be predicted...”, the report says (Report, p.27). None of these issues, the report says, involve malicious code: “There were no instances discovered of any intentionally malicious code having been written by the vendor and included in the voting system source code.” (Report, p.27).

8. DOUBTFUL ESCAPE CLAUSE. Whenever it refers to what seem like major concerns, like those cited in this paper, the Report waffles by inserting or appending with almost regular monotony an escape clause like the following sentence(s):
“Given the testing done to date without corruption issues being raised, would indicate that the risk is minimal in a normal path of execution... The implementation of manual processes and procedures will further mitigate any potential issues.” (Report, p.15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 31)

In fact, in some parts where they are inserted or appended, it was apparent from the altered format of the document that this was done so as an after-thought, i.e., after the main body of the document had been written. We have received information from some Comelec insiders that “a series of letters were exchanged between the Technical Evaluation Committee and SysTest regarding some of the major concerns raised by SysTest and requests by the Philippine side for changes in the report tone and language.” This is corroborated in the Report, whose revision history (Report, p.2) shows that it was “submitted to the COMELEC for review” seven times. It seems irregular that the COMELEC was itself “reviewing” what is supposed to be an independent review. It is suggested in the interest of transparency that the COMELEC likewise release to the public this series of letters, just as it released this Report. Earlier versions of the Report should also be released for scrutiny. They can reveal how the Report changed in the course of the “review” by the COMELEC.

**9. POSSIBLE DATABASE CORRUPTION.** The Report has warned of the possible corruption of the election database by the central count software, as follows:

“The logical order of instructions that may be executed in response to unforeseen exceptions being encountered during execution of the vendor's central count software is non-standard and, as written, may result in database corruption.” (Report, p.16)

Prior to this, SysTest admitted that the review it conducted, which was a static review, could not settle the matter:

“It, therefore, cannot be determined through static source code review whether any actual database corruption will necessarily be the result.” (Report, p.16)

When a file or database is opened for use, it is assigned a unique number called a “handle”. All subsequent accesses to the file or database is done through its handle. File and database corruption can result from the improper management of file and database handles, as cited by the Report below:

“When a program makes use of an external resource, such as a database or a file, a 'handle' to the resource is created.... Instances were found in the source code of handles being created and not closed at all. In other instances the close statement was found within the body of the try block positioned such that it would not be executed in the case of an error being encountered above it within the try block. In many instances, there are no enclosing try blocks. In those cases, not only will the handle be left open if an error occurs, but no provisions are made to handle any possible errors.” (Report, p.24)

If vote data is corrupted, and transaction logs are at the same time lost (see the next problem), it may not be possible to recover the vote data that was lost. Undetected corruption of vote data is another
scenario, which can lead to the proclamation of winners based on corrupted vote data.

10. POTENTIALLY INCOMPLETE, CORRUPTED, OVERWRITTEN OR LOST AUDIT LOGS. The Report warns of potential problems in the audit logging subsystem. These problems could lead to failure to log important events or their time of occurrence as well as to corruption, overwriting, or loss of log entries or log files. Such problems can make it impossible to trace back problems and conduct forensic studies, in case this should be necessary. They can also make it possible for intruders to hide their tracks. The Report identified sections where logging functions do not log the time of occurrence:

“Several of the logging functions in the Smartmatic CCS project appear to omit the inclusion of the time and date from the logged messages. These functions are accessed throughout the system as logging functionality is required. This apparent omission may result in audit log entries without complete data and time information being included as part of each individually logged message.” (Report, pp.18-19)

... “The main audit logging function does not include the time and date in the logged message. This function is widely used for logging audit messages throughout the system, and will result in audit log entries without complete time and data stamps associated with each message.” (Report, p.23)

The Report found that some important – in fact, critical – events are not logged:

“Numerous instances were found in which the display of error, informational, or confirmation messages presented to the user, and the user responses to those messages, were not logged. It also appeared that not all machine-generated error and exception messages will result in the creation of audit log entries, and not all critical system status messages displayed to the user by the system during the course of normal operation will be logged. Additionally, it could not be confirmed through source code review that every non-critical status message generated by the machine's data quality monitor functionality, or by software and hardware condition monitors, will be logged.” (Report, p.19)

... “... it was determined that not all critical system status messages that are displayed to the user by the system during the course of normal operations are written to the audit log.” (Report, p.23)

... “Numerous instances were found in the source code in which the displays of error, informational, or confirmation messages to the user, and the user's responses to them, do not generate audit log entries. It was also determined that not all machine-generated error and exception messages result in log entries, and not all non-critical status messages generated by the machine's data quality monitor or by its software and hardware condition monitors are logged. (Report, p.23)

The Report warns that logging may be disabled or audit logs may be moved or overwritten:
“The EMS [Election Management System] does not provide measures to protect against tampering during maintenance activities.... In at least one instance, an audit log was able to be moved without an alert or stoppage from the system.” (Report, p. 30-31)

... “It was determined that output to an audit log file may be disabled by the setting of a quietness parameter. It also appeared that multiple entities may have the possibility of writing to a single log file using class method logFile.LogMsg() without clear controls over ownership of the file handle, or clear comments indicating that that is the single audit logging thread. If multiple instances of the logFile class have the same log file open at the same time, then the class instance that saves changes to the file last may overwrite all previous changes made by the other class instances.” (Report, p.21)

“EED [Election Event Designer] does not provide measures to protect against tampering during maintenance activities. The documentation does not provide procedures for safeguarding the audit logs.” (Report, p.31)

It also found that test runs were not logged. Thus, problems, failures and other important events that occur during test runs are not recorded. During Smartmatic field tests and mock elections, for instance, we could have accumulated significant test data that could help measure failure rates, rates of rejection of valid ballots, and accuracy rates under field conditions, had such logs been available. The Report says:

“The reviewer was unable to find adequate evidence of logging of a run of test ballots. The VVSG requires that the auditing log contain a record of the number of test ballots sent, when each ballot was sent, the machine from which the ballots were sent, and the specific votes or selections contained in the ballots. The SysTest reviewer was unable to verify the existence of specific reference to the logging of any of these items.” (Report, p.21)

The Report warns that some functions during transmission may not be logged, including the identity of the contacted wireless device or if and when a disconnection is made:

“The reviewer was unable to verify that the identity of the contacted wireless device was logged when the resident device made a connection. The reviewer was also unable to find any function that logged the disconnection of the wireless device. Specific functions involved in the disconnection were found and examined, and it was determined that these functions did not include the logic required to log their activities.” (Report, pp.21-22)

11. POSSIBLE INJECTION OF MALICIOUS SQL COMMANDS. The significant security hole which can allow “malicious” SQL commands was identified by the Report:

“It is possible to bring about other than the normal and expected database activities, potentially exposing a database to possible corruption, by the submission, or injection, of malicious user-entered Structured Query Language (SQL) commands.... there are possible susceptibilities to SQL injections within the Dominion EMS. While the EMS source code does generally
implement the prescribed protective measures throughout the code, several instances were found to exist in which user-entered data-related commands may be submitted to the database in such ways that the implemented protective coding may be bypassed.” (Report, p.19)

12. UNENCRYPTED PASSWORDS IN DATABASE AND OTHER ENCRYPTION AND PASSWORD PROBLEMS. The Report warns against plaintext passwords being stored in the election database:

“It was discovered that the possibility of unencrypted passwords being stored in the EMS database may exist in the Dominion EMS. It appears that the problem logic as implemented does not call for the encryption of user passwords when storing them in the database.” (Report, p.19)

“It was also determined that, in at least one instance, encryption keys were found to be explicitly coded into the source code of the system. That encryption keys were discovered within the source code could potentially make them available to anyone that might have access to the executable binary version of the EMS application.” (Report, pp.19-20)

“... data may not always be properly encrypted before being stored. It also appeared that Certificates of Canvass and Statements of Votes documents may not always be encrypted before transmission.” (Report, p.24)

The Report also found that part of the software simply did not allow entry, unless the reviewers bypassed the validation system and used a work-around, which introduces a security issue:

“The [Canvassing and Consolidation] system did not allow entry, until a work around was introduced that in effect turned off a token validation that regulates entry into the applications. This is an issue with security ramifications to the system.” (Report, p.29)

13. POSSIBLE LOSS OF SIGNIFICANT DIGITS. The Report also found instances of “mixed mode operations” where numeric data are converted from one type to another, resulting in possible loss of significant digits.

“Instance of mixed mode operations, the usage in mathematical calculations of values converted from one declared numeric variable type to another, were also found within the Dominion EMSs source code. Mixed mode operations may be risks involved if the value being converted is of a floating type, and it is converted to a decimal type, thereby potentially losing precision, or if the type being converted is assigned to a type implemented as a smaller variable type, in what is known as a narrowing conversion. Narrowing conversions may result in a loss of value of the resultant type is not capable of containing the value of the variable subject to conversion.” (Report, p.20)

Like the “narrowing conversion” above, overflow problems cited by the Report below can also drop digits from vote counts:
“A few instances were found where the source code did not include checks for the possibilities of vote count variables being overflowed. Numeric overflow is possible if the value assigned to the variable becomes more than the maximum permitted value for the numeric type of the variable. The risk can only become manifest if a large number of votes are processed through a single PCOS.” (Report, p.22)

14. NON-SMARTMATIC SOFTWARE PACKAGES AS WELL AS COMPILER AND LIBRARIES NOT PROPERLY REVIEWED.

“There is a list of the required COTS [Commercial-Off-The-Shelf] and open source software packages, including providers and versions, required to build the Smartmatic EMS and CCS applications. The current inventory list provided by Smartmatic has proven to be inadequate. This indicates that vendor may lack the formal configuration management procedures expected to be in place.” (Report, p.25)

For compiled packages, such as the PCOS software, the compiler and its libraries should have also been reviewed, because malicious code may be introduced not in the main body of the software but in the software libraries or even the compiler itself, if it is a non-standard compiler. This review was not done. So the possibility of malicious code introduced from libraries or compilers cannot be ruled out.

15. FAILURES RATES, BALLOT REJECTION RATES, AND ACCURACY RATES NOT TESTED OR MEASURED. The Report did not describe any detailed testing to determine PCOS failure rates, rates of rejection of valid ballots, and accuracy rates. These essential measurements could have been done under the SysTest system audit, the full report of which has not been publicly released by the COMELEC.

16. WAS ADDITIONAL IN-DEPTH REVIEW DONE? The Report recommended that “an additional in-depth review be performed when possible”. The COMELEC needs to confirm whether this recommended review was conducted and to report to the public the results of such a review. The immediate basis for this SysTest recommendation was the following highly damaging finding:

“The pattern of miswritten exception handling and erroneous transaction terminating logic is so widespread that it appears that the system authors used an incorrectly written template for such source code logic, and that the incorrectly written aspects of the template have resulted in potential exception handling errors everywhere that the template may have been used. A number of such instances were individually described to the vendor by SysTest, and subsequently addressed by the vendor, but the vendor made no effort to correct any such constructs not specifically identified for them.” (Report, p.15)

17. SMARTMATIC SOFTWARE NEEDS A LOT MORE DEVELOPMENT WORK AND THOROUGH TESTING. Systest found a total of 9,319 deviations from standards and another 569 non-standards-related issues that generated concern. Of the 9,319 standards-related issues, 4,422 were “critical” or “major”, which Smartmatic has reported “resolved” and which SysTest therefore “closed”.

8
However, the software modifications that resolved these “critical” or “major” concerns have not been successfully tested or even piloted here or abroad, and 4,897 “minor” issues remain to be resolved. Even these so-called “minor” issues, when scrutinized, turn out to be significant, with the SysTest language possibly toned down. Of the 569 non-standards-related issues, all of which remain unresolved, 327 are “major” and 242 “minor” concerns. All these suggest that the Smartmatic software still needs a lot of development work and thorough testing before it can be successfully deployed.

A clear indication of the sorry state of the Smartmatic source code was the high number of simple programming errors that SysTest reviewers found in the Smartmatic code base:

“SysTest's reviewers did, however, find a wide array of basic programming errors in the Smartmatic source code; errors of uninitialized object variables being accessed, errors of variables explicitly being initialized to default variables and then immediately being tested in conditional expressions for the presence of some other value, errors of not capturing the values returned from called functions, and other basic programming mistakes that should give the reader pause to consider the extent of internal quality control measures that the subject code may have been subjected to prior to submission to SysTest.” (Report, p.27)

18. WERE ALL COMPENSATING CONTROLS ACCOMPLISHED? To remedy the problems that SysTest identified, it subsequently submitted a separate report entitled “Final AES Certification Test Report for the Smartmatic Automated Electon System (AES)”, which the COMELEC has not yet made available to the public, although it has released a summary of the report, dated March 8, 2010 and entitled “Certification Test Summary for AES May 2010 Rev. 1.00” (henceforth called Summary). The Summary lists “compensating controls” needed to cover the shortcoming in the Smartmatic software identified in the Report. In particular, two compensating controls listed in the Summary should be noted (Summary, p.6):

“- The Ballot Production tool was not subjected to the full certification process; therefore it should not be utilized in the May 10, 2010 election process.”

“- As the modem firmware was not subjected to the full certification process and is required for transmissions, COMELEC should request the source code from Smartmatic and have a thorough review conducted prior to the May 10, 2010 election.”

Given the transmission problems encountered by Smartmatic even in Metro Manila and the printing problems of the NPO with regards to misalignment from high-speed printing, these two compensating controls seem particularly important. The COMELEC should report to the public whether these two, as well as the rest of the compensating controls listed in the Summary, were accomplished.

Accomplishing the compensating controls is particularly important because of the conditional endorsement by SysTest contained in the Summary (p.7):

“Assuming the abovementioned [compensating] controls are put into practice and that the AES is properly configured, operated and supported, SysTest Labs finds the Smartmatic Automated
Election System to be capable of operating properly, securely and accurately and therefore recommends the system for certification and use in the May 10, 2010 election.”

This is not quite the categorical statement that the AES Law R.A. 9369 requires. This endorsement is conditional on the crucial assumption that all compensating controls are “put into practice”. So, the COMELEC definitely needs to clarify the status of implementation of the compensating controls.

19. NO CERTIFICATION SHOULD HAVE BEEN ISSUED. We believe the COMELEC and its Technical Evaluation Committee (TEC) erred in interpreting the Report as a categorical endorsement that the AES was working properly, securely and accurately. Given the warnings cited above, we believe they seriously erred in ignoring the warnings contained in the Report and in pursuing what is in fact a high-risk project of converting from a fully manual to a fully automated system within a single election cycle, despite the clear requirement of the AES Law for a pilot project.

In effect, the SysTest system audit and source code review benefitted Smartmatic more than the COMELEC. Smartmatic obtained invaluable information from SysTest about 9,888 problems in its software suite and corresponding suggestions and advice for improving the software for future clients. The COMELEC chose to ignore the warnings of the system audit and code review, for which it paid P72 million (1% of the total AES project cost of P7.2 billion), exposing itself and the whole country to the risks associated with problematic untested software.

In effect, too, we are paying Smartmatic P7.2 billion for the dubious privilege of serving as their guinea pigs for testing the recently-modified Smartmatic software that is saddled with unresolved “major” and “minor” issues as well as “critical” and “major” issues which, although resolved at the static software review level, has never been field-tested anywhere.

20. HALAL RECOMMENDATIONS. To mitigate the impact of potential software problems on the automated May 10, 2010 elections as well as facilitate post-mortem analysis, Halalang Marangal recommends to the COMELEC the following measures:

- Allow public access to the original copies of the SysTest reports, to settle issues of authenticity, and make public all documents related to the SysTest system audit and source code review, including official letters exchanged between SysTest and the COMELEC or any of its committees, earlier versions of SysTest reports, especially before these were revised after COMELEC review, analyses and inputs contributed by other local bodies like the Department of Science and Technology (DOST) and international bodies and their consultants, like IFES.
- Remove existing restrictive conditions for the review of the Smartmatic source code by local reviewers and extend to the latter the same terms and conditions as those granted to SysTest.
- Ensure the full implementation of the compensating controls recommended by SysTest.
- Adopt more recent international standards for electronic voting systems and make them mandatory.
- Tap local expertise in conducting a post-mortem system audit and source code review.

Roberto Verzola, Halalang Marangal (HALAL), 2 May 2010