INDEPENDENT TECHNICAL TEAM REVIEW REPORT – VERSION 4.0

Summary of study conducted by independent technical team

Developed By - KAK

TABLE OF CONTENTS

Introduction

The evaluation on Electronic Voting Machine was done based on the request received from Mr. V V RAO, convener election watch and Vice President JANA CHAITANYA VEDIKA.

Our Engineers were involved in developing a simulated product in similar lines with the features of the Electronic Voting Machine with a Control Unit, and a Ballot Unit. And have performed extensive research to understand how vulnerable the Electronic Voting machines are.

The following questions are the outcome of the Evaluation done:

Questions – On Process

1. Was the chip used a generic chip or specifically designed ASIC chip to be used only for Electronic Voting Machine?

2. What is process involved in the procurement of the chip & who are the people involved in that process?

3. Does the Election commission have the information on procurement chips & the process involved?

4. Is there any encryption in the Ballot unit used for transfer of the data to control unit, if so what is the encryption and what is the software used in the Ballot Unit for enabling such encryption?

5. Have the old machines been replaced, and how many more old machines have been used and can we obtain the manufacturing dates, batch numbers, serial numbers including the life of each of the Electronic Voting Machine used in the recent elections held?

6. Who are people involved in maintenance of EVM, are they permanent employees of ECIL / BEL or are there any contract labor involved?

7. In the recently concluded Elections, how many of the machines failed to read the E2PROM, & in case of memory becoming unreadable, what are the alternate methods adopted?

8. What does Election Commission do with the faulty machines, if they are repaired what is the process and who are the people / organizations involved, is there any Annual Maintenance Contract for the Electronic Voting Machines?

9. Is there any form of Randomization involved before EVM's are being sent to the Districts for first level randomization?

Questions – On Expert Committee Report

1. Was the Chip used an OTP (Where the code is fused in house at the manufacturer's location) or Masked ROM (Where the code is sent outside the country to be fused into the chip at the vendor's location)?

2. Are the CU & BU cards sealed as suggested by the Prof. INDIRESAN committee report?

3. How can a Ballot Unit Encrypt the data while transferring data to Control Unit without software and as everyone knows we need a microcontroller for loading this software?

4. What are the modifications & upgrades suggested by the Expert Committee that were developed by the manufacturers in the Electronic Voting Machines?

5. How many Electronic Voting Machines used were upgraded in the election held recently?

6. Is there a self test signature for every Electronic Voting Machine?

7. Did the Election Commission take the complete print out of every key pressed wherever there were incidents of Mal-Functioning of Electronic Voting Machines? As Expert Committee insisted on Data & Time Stamping every key pressed.

8. Why did Election Commission disregard the suggestions made by the Expert Committee in regards with the modifications & upgrade of the Electronic Voting Machines used in the elections held recently?

Questions – Technical

1. What are the specifications of Hardware, Firmware & Interfacing?

2. What are Standards & Guidelines followed while coding?

3. What are Standards followed for designing the Hardware?

4. What are the standards followed in designing the Encasings?

5. What are the Certifications available for Hardware?

6. What are the test cases & reports of the entire project?

7. Was any Risk Analysis performed?

8. What is methodology of Full Load test?

9.   What are the fail safe parameters for Firmware, Hardware as well as Interfaces?

10. Was any Disaster recovery mechanism adopted?

11. Is the Hardware unit capable of interoperability, to avoid monopoly & vendor Lock-In?

12. What kind of encryption is used for data security?

13. What is the Complete Operational Process of CU & BU?

14. What are the MTBF (Mean Time between Failures) of various components used?

About Electronic Voting Machine

The Electronic Voting Machines (EVMs) are now pressed into service to conduct elections for Lok Sabha and State Legislative Assemblies by the Election Commission of India, replacing the time tested ballot box system of the past. The EVM system consists of three hardware sub-systems and one software system, namely:

(i)   Control Unit.
(ii)   Ballot Unit.
(iii)   Inter-connection Cable between Control Unit & Ballot Unit.
(iv)   The Source code / software Programme embedded in the microchip in the Control Unit.

On the Voting Machine, there will be a fixed ballot paper with the names of the candidates of the respective Political Parties with their Party Symbols. A Green Light will be on the Ballot Unit which indicates that the Unit is ready to receive the vote. When the voter enters into the Polling Booth and when he presses the button against the name of the candidate whom the voter wants to vote, a Red Light (LED) will lit itself indicating that the Unit has recorded the vote and the Green Light will be automatically off. At that moment, a beep sound also comes out of the Control Unit and the Red Light (LED) will be off automatically. This is the process involved in giving us an indication that the voter has exercised his franchise as desired by him. The process of voting goes on these lines under the supervision of Presiding Officer. At the end of the poll, the Presiding Officer presses the button indicating the closure of recording of the votes in the Control Unit and seals the Unit. The process in the

Electronic Unit is such that the voter does not see what is happening in the other part, which is called the Control Unit (CU). When the voter presses the button, the vote is recorded in the 2nd Unit which is connected to the Ballot Unit. The technology involved in this process is such that the voter cannot know whether his vote is registered in favor of the candidate he intended to vote.

At the time of counting, the Control Unit is brought and after the seal is removed in the presence of the agents, the Counting official presses the button meant for counting. After he presses the button, the result is displayed in the sequence beginning with the total number of votes and subsequently, total number of candidates, then the votes recorded against the serial number of the candidate in a time sequence. The totals displayed in the machine against each candidate are recorded by the official and by the election agents who are present there. These are totaled after the counting and the result is announced.

Origin and Development

According to information available, the Electronics Corporation of India (ECIL) developed these Electronic Voting Machines. The Company used 8 Bit Chip (8 Bit Microcontrollers). The complete Research and Development of software took place in ECIL. After developing the Code, it is believed to have been sent to a selected Company, Hitachi (now RENESAS) in Japan for fusing the code into the Chips. As per the existing data, ECIL the manufacturer of EVM has utilized 8 Bit Microcontrollers called the chip across this document. Post the complete research & development within ECIL the source code developed was sent to the Vendor (RENESAS) in Japan for being fused in to the chip. The mode of sending the source code could be through the distributor of the vendor in India, and the process of sending it securely is not known. Generally the Source Code will be sent through a distributor of the Company in India. It is not within our knowledge whether the process of sending it through a distributor or otherwise is a guarded secret or not. In this process, there is every possibility for swapping of the source Code and insertion of a 'Trojan' into the source Code and sent as a substitute to the original Code. This can be automatically activated if and when required at any subsequent stages. Similarly BEL another manufacturer of the Electronic Voting Machines has used MICROCHIP vendor's chip inside their Voting Machine, and also have adopted similar process as mentioned above for fusing source code into the Chip.

After the Manufacturer makes these Chips as per the modified Code, they are shipped back to the ECIL or BEL, who in turn plant these chips into the Voting Machines of their make. The process of shipment of the Chips from Japan involves various stages of clearance. The Chips are delivered to the distributor in India and the distributor hands them over to either the ECIL or BEL. Chips are custom cleared in India through Clearing Agent. There is no idea as to the reliability, security and integrity of the Agency.

There is also another way through which the Chips can be procured from the same Manufacturer with the original Code along with the Trojan in it through the distributor or his agent or some other means. These Chips with the manipulated (altered) Code can be delivered to the Manufacturer of the Voting Machine as if they are of the original Chips. It is not known who have access to the processing of the Code at various stages of its formulation. The intricacies and the persons involved in this process of manufacturing of Chips and formulation of Code is a matter to be investigated into very deeply. It may be mentioned that there is no mechanism or method by which it could be verified whether the Chip manufactured and used in the voting machines contains the original Code or not.

Expert Committee Review

The expert committee headed by Prof. INDIRESAN had suggested the following upgrades to the Electronic Voting machine before the voting machines can be used for the 2009 General Elections on the 5th of September 2006, and they are as follows:

- ➢ **EMV's be EMI/EMC Compliant**
- ➢ Dynamic coding of key no's to enhance security of data transmitted from the Ballot Unit (BU) to the Control Unit (CU) be introduced
- ➢ Time diversity in data recording be introduced to eliminate effects of random noise.
- ➢ Every key press on EVM, even if invalid, is date-time stamped and kept as permanent record.
- ➢ **Additional seal of electronic cards in CU, BU may be introduced by EC to be operated just before the candidate-list is declared as per 3.4e.**
- ➢ All the instruments are checked as a matter of preventive maintenance before election and as a matter of abundant caution, to ensure that they are working satisfactorily and **according to the original embedded program.**
- ➢ The battery condition should be in MEDIUM or HIGH at start of election as displayed on the EVM.

> ➢ It is ensured in every polling booth that the cable is visible all the time.

> ➢ At the time of the insertion of the cable it is formally recorded by the Presiding Officer and the polling agents, that no device has been inserted between the cable and the connector

> ➢ After the polling, the cable and Balloting unit is physically inspected for any mechanical damage, or seal intact.

If only few of the above-mentioned upgrades were developed and demonstrated by the manufacturers of the Electronic Voting Machines to the Election Commission then it means that the Voting Machines used are not upgraded so **are not stable & are not secure and should not have been used for the conducting free & fair elections**.

Issues on Expert Committee Report

All through the executive committee report the major issue raised by most of the people i.e. tampering of the Electronic Voting Machine has not been technically addressed. Further we have noted that the answers provided to the above-mentioned problem are not technically clear.

Issues observed from the Executive Committee report on Electronic Voting Machines are quoted hereunder:

Point no# 3.4 issue no# (a) states that the chip used is an OTP i.e. it is programmed by the manufacturer and not by the vendor.

But if this is the case why are Masked Chips used, which means that the source code was not fused in India at the manufacturer's premises under stringent security but it was sent over to the vendor outside our country, and were delivered through various delivery channels to the manufacturer and so can be prone to any kind of tampering at various stages of the shipment.

Point no# 3.4 issue no# (c) states that the unique ID mates to the E2 PROM (within the CV where all the voting data will be stored during an election) and, the micro-controller, at the instant of first power-up,

of the CU at the time of manufacturing. Subsequently, the CV will not function if the ID stored in the

micro-controller memory does not match that in the E2PROM. Thus any item to modify the data stored

in the E2 PROM by replacing the E2 PROM will automatically make the EVM inoperative.

As the entire lot of the E2PROM shall have the same Unique ID and this also has to be sent along with

the source code to the vendor for fusing into the Chip, there is always a possibility of Trojan being added

into the chip with the E2PROM ID already existing. Adding to this there are more than one instances of

the E2PROM being replaced while the polling operations were being conducted due to the

malfunctioning of the E2PROM, and this as per the Committee report should have made the EVM

inoperative?

Point no# 3.4 issue no# (d) first & second paragraph states that there is no possibility of a Trojan horse

Furthermore there is no evidence of mentioning of the fact on how many number of EVM's were

upgraded with the modifications suggested by the committee as well as how many old EVM were reused

for this elections at any point of the document.

As the software changes or modifications that were accepted by the manufacturers is not possible to be

implemented in the existing hardware design as the chips used are Masked Chips and are technically

unalterable and also this has been accepted by the Honorable Committee in the report. These changes

require a complete New Circuit Board with a New Chip mounted on it with the proposed additional

modifications to the software.

Even if we believe that few EVM's were upgraded with the suggestions of Dynamic Key Coding the, with

all due respects to the technical committee, we would like to inform that though the program is capable

of recording every key pressed, still it's quite very simple to have a key sequence when pressed activates

the Trojan and go unaccounted / un-recorded and this a very simple mechanism in the code and is not

rocket science. There is a possibility of simple coding mechanism, which can state that whenever Key

1,2,3,4 Etc., for example, are pressed in sequence, not to record any of these keys as well as activate the

Trojan. Only way to prove that there are no Trojan is opening the source code to third party vendors for

testing. Considering the number of keys on the EVM BU to be 12 then there are possible 12!

Permutations & combinations of keys totaling to 47,90,01,600 i.e. around 48 Crore Key Sequences, now

to test each of the Electronic Voting Machine with such a number of key sequences would be highly

impossible. Thus the mock test performed is not thorough enough to disprove the fact of activation of

Trojan existing in the source code of the EVM.

Point no# 3.4 issue no# (e) Adoption of a seal on Circuit Boards in from t of the party representatives for

ensuring that there is no swapping of the CU circuit boards possible.

Though the suggestion is very appropriate, still none of the Control Unit Circuit Boards were sealed, and

no there is no such mention of a modification to the existing Ballot Units.

Point no# 3.5 issue no# (i) & (ii) & 4.6 issue no# (V) states that Data can be fed to CU only through BU.

Special Encryption is used in passing the data from BU to the CU.

Once again technically it's not clear how can any embedded device without any processor or micro-

controller or any chip transfer data with encryption. As a matter of fact any encryption is an advanced

program that encodes the data into something that cannot be decoded by anybody for security

purposes. But if there is no chip on the BU then it shall only be a simple RS 485 cable that sends plain Key

Code over the cable to the CU as an input. And this can be tempered at any stage.

Point no# 3.6 In this manner, the committee to the best of its ability has looked into all possibilities of

tampering with the EVM and has come to the conclusion that there is no way of altering the results of

the polls before, during and after the poll duration provided, due security precautions already in force

and additional modifications suggested by the committee are enforced and the sealing at various stages is adhered to. & **Point no# 3.7** In view of all these factors, the Committee' unanimously certifies that the EVM system is tamper-proof in the intended environment when due precautions are taken. For these reasons, the Committee recommends that the upgraded EVM with suggested modifications, testing and operating precautions may be accepted and put to use.

There has been no evidence provided to support the fact that the suggestions made by the expert committee were followed subsequently.

Point no# 3.8 states that as a preventive measure, the Committee recommends that before every election the manufacturers may be asked to check (this can be done very fast through a very simple exerciser) and ensure that all the units are functioning as designed. Incidentally, this method will be checked, by what is called 'the self test signature of Machine' and thereby the Manufacturers will be able to certify that the Machine is identical to what they have supplied and it has not been modified or replaced by any other.

There has been no evidence provided to support the fact that the suggestions made by the expert committee were followed subsequently, as observed by petitioner's in their election watch as micro observers of the recent elections.

Point no# 3.9 the expert sates to accept the Electronic Voting Machines for polling only if all the suggestions are followed.

The suggestions are not completely followed by the manufacturers leaving enough room for security breach, which was also the main cause of concern of Executive Committee.

Point no# 4.6 issue no# (b) states that the Expert Committee has advised a Date & Time Stamp to be implemented on every key pressed

This obviously means that the Voter pressing the Key on the ballot Unit is also recorded along with date & Time Stamp, which can be mapped to the manual register available with the polling agents where all the voters are supposed to sign or put in a thumb impression before voting. Thus knowing the time of the first voter from the EVM and mapping it to the register can actually bring out the detail of the vote casted by every citizen. This puts our democracy into a major threat as the secrecy of the ballot is lost.

Point no# 4.7 states that EVM is factory Masked; again the response is very ambiguous as they have mentioned in the point no# 3.4 issue no# (a) as OTP and now they mention it as Masked.

We really would like to get a clarification on the same, whether the chip used was an OTP or Masked Chip, as the expert committee states that the chip used is an OTP in the point no# 3.4 issue no# (a) and the same is mentioned as a Masked ROM in the point no# 4.7. It has to be noted that there is a significant difference between an OTP & a Masked ROM as the code can be fused into the chip inhouse i.e. at the manufacturer's location if it is an OTP and if it is Masked ROM the code has to be sent to the vendor in Japan for being fused into the Chip.

Point no# 6 section no# (i) states about the recommendations that the EVM Manufacturer has to abide

There has been no evidence provided to support the fact that the suggestions made by the expert committee were implemented subsequently.

Point no# 6 section no# (ii) & issue no# (a) states that there is a possibility of electrical check of the Control Unit & the Ballot Unit prior to polling.

There was no diagnostic check available for checking the sanctity of the embedded program in the EVM as observed by the petitioner as a micro observer of the recent elections. Neither the technicians, who prepare the EVM's for elections, understand the recommendation made by the technical committee.

Possible Manipulations

With the details mentioned above the following are the areas of key concern where the electronic voting machines can be manipulated. The points mentioned below gives an insight to the possible manipulations with the Electronic Voting Machines.

The source code / programme software developed for the electronic voting machines locally by the manufacturer was either uploaded through Internet or was sent through a courier to the concerned distributor of the chip vendor in form of a CD. **There is no secured methodology adopted for the transfer of thus developed source code / programme software** to be fused in to the chip, thus creating a possibility of the source code / software programme being swapped with new source code, which has Trojans.

The chips are delivered from ex-Warehouse picked by a courier or logistics agency appointed by the distributor of the chip vendor, cleared at the customs and delivered to the Manufacturer of EVM's without much security. The above process provides a grave opportunity of **replacing and manipulating thus procured chips at various levels of shipment.**

The only way of identification or verification of thus received chips from vendor being original or authentic is the Chip ID provided by the vendor. **There is no verification program developed to cross check every chip for genuine code** before mounting on to the circuit board (EVM Control Board). And no manufacturer is in a position to define whether the Chips are original due to lack of a thorough verification tool.

Ballot Unit can be swapped at any point of time as **there is no encryption between Ballot Unit & Control Unit** except claiming a proprietary protocol that is nothing but a simple RS485 communication, which is open to any sniffers. A new Ballot Unit can be attached to the Control Unit. This throws open immense opportunities for running Trojans and even mount receiver circuits on the circuit board of the Ballot Unit enabling it to be controlled remotely to activate the Trojans.

Manipulations – Pre-Poll

After the withdrawal of candidates for a constituency, the allotment of keys on the Ballot Unit is done through the Control Unit by pressing the "CANDIDATE SELECTION" Button. The Trojan can be activated to favor a particular key by means of adding percentage over other key or by deducting a set of votes polled for all other keys and adding to the favored key. It cannot be detected at the Mock Test as there are various methods of activation like Time based, Minimum Number of Votes Polled, Power on Reset (By Switching off / on the power of EVM) Etc., after the voting process.

Manipulations – While-Poll

Trojan can be activated by anybody going in as a voter entering the sequential key code on the Ballot Unit. This can go absolutely undetected as the buttons pressed in that sequence cannot be captured nor produce any beep sound, because of the functional behavior of the Trojan.

Few Facts to Mention I

As reported in Hindu dated Wednesday, May 06, 2009.

CUTTACK: Re-polling in hypersensitive Nimasahi booth under Cuttack-Barabati Assembly segment witnessed volatile situation when tempers ran high. Police had to resort to lathicharge twice in the day to quell warring groups who had gathered outside the polling booth.

Unconfirmed reports indicate that at least five persons, including a policeman were injured when resorted to lathicharge to chase rival party workers. Re-polling in the booth was necessitated by allegations of EVM tampering on April 23.

District election officer Kishore Kumar Mohanty later in the evening said the re-polling went off peacefully barring the mildlathi charge. At least 64 per cent of polling was recorded in the booth, he said. Polling began smoothly in the morning and by 9 am at least 30 per cent of 998 voters had exercised their votes. But trouble began around 11 am when Congress leaders became restive alleging that rival party leaders were wooing the voters inside the booth. Soon the gathering gained numbers and there were heated exchanges among BJD, BJP and Congress workers.

Sensing trouble, police swung into action chasing groups, thrashing trouble makers. City DCP A N Sinha also arrived at the spot and brought the situation under control. Polling then started smoothly and by 1 pm 53 percent of voters had exercised their franchise.

But around 4 pm, trouble again reappeared at the booth when supporters cutting across party lines started rumbling about the morning's police action. But acting swiftly once again, police brought the situation under control and ensured that the polling ended peacefully at 5 pm.

Conclusions I

There are possibilities of the EVM get malfunction due to Trojans insertion.

Few Facts to Mention II

In the Constituency of Khammam (Khammam Dist), Polling Station# 198, the total number of Votes were 1039 and actually polled were 644 at the round no:17, table no: 6 and the Serial Numbers of Central Unit (CU) : A 54199 & Ballot Unit (BU) : F 10996. In the above booth **the Electronic Voting Machine could not read data** and **the votes were discounted** by the EC officer. As per booth data collected from Dist. collector office, this particular booth data is missing in the report.

Conclusions II

When Electronic Voting machine is vulnerable i.e. if the Electronic Voting Machine Chips are swapped the Electronic Voting Machine can be manipulated as above-mentioned scenario in the section Few Facts to Mention I. Further whenever the Electronic Voting Machines can be manipulated they can also provide the scope for misbehaving & technically they tend to overflow the buffers available in the Control Unit for execution thus the Electronic Voting Machine tends to get hanged, a similar scenario to that of a virus infecting the Windows Desktop. **Manipulated Electronic Voting Machines can misbehave and corrupt the entire memory as well as hang the Control Unit and thus rendering the E2PROM unreadable.**

Few Facts to Mention III

In the Constituency of Pedakurapadu (GUNTUR Dist), Polling Station# 2 & Booth No# 2, 122 Votes were polled in the First Electronic Voting Machine malfunctioned and further **as the Electronic Voting Machine mal-functioned** and was replaced by a second EVM by the officer.

THE REPLACED SECOND EVM VOTE COUNT		
SNO	Party	Votes
1	INC	186
2	TDP	176
3	PRP	34
4	IND	18

Total	414

Conclusions III

The First EVM had registered a total of 122 cotes and as the Electronic Voting Machine at the time of results declaration malfunctioned the votes could not be read from the EVM and have been forfeited. This leads us to a conclusion that the **Electronic Voting Machines are not stable** as declared or mentioned by the Election Commission and so are not fail-safe for being used in the elections. How can a vote cast by a citizen of India in a democratic country be forfeited?

Few Facts to Mention IV

List of Booths where the machines could not read data

AssCode	BoothCode	AssName	BoothName
23	60	Ramagundam	Medipalli
23	61	Ramagundam	Medipalli
70	197	Secunderabad	Osmania University
80	60	Alampur(SC)	Ieeza
80	69	Alampur(SC)	Ieeza
84	128	Shadnagar	Kesampet
104	185	Parkal	Katrapally
104	197	Parkal	Nallabelly Yelugur
104	209	Parkal	Semgem
104	212	Parkal	Gavicharla
104	221	Parkal	Bollikunta
104	224	Parkal	Ramachandrapuram
112	198	Khammam	Kothagudem
198	142	Vijayawada West	Mallikarjuna Petta
231	31	Giddalur	Kandulapuram
240	250	Sullurpeta (SC)	MPP School Ramapuram Kuppam
257	44	Panyam	Bollavaram
257	45	Panyam	Bollavaram

Conclusions IV

The above issues indicate a significant fact that the Electronic Voting machines were not tested thoroughly and have been put to use. As a matter of fact the Electronic Voting Machines have not functioned properly in the above-mentioned polling booths where the Electronic Voting machines were replaced for the purpose of Polling**. This piece of information provides evidence & concludes that the Electronic Voting Machines can malfunction and are unstable and further EVM's are not Fail-Safe as mentioned by the Election Commission of India.**

Few Facts to Mention V

The below table shows the list of polling booths where there was a particular pattern of voting as per

SNO	ASSEMBLY	MANDAL	PANCHAYATH	Booth	TOL	TDP	%	INC	%
1	Rajam (SC)	Vangara	Vangara	30	11	0	0	11	100
2	Yerragondapalem	Dornala	Dornala	135	27	0	0	27	100
3	Jammalamadugu	Jammalamadugu	Gandikota	120	555	0	0	555	100
4	Jammalamadugu	Jammalamadugu	Goriganur	75	712	0	0	712	100
5	Jammalamadugu	Jammalamadugu	Dharmapuram	74	458	0	0	457	99.8
6	Jammalamadugu	Jammalamadugu	Devagudi	69	776	0	0	774	99.7
7	Jammalamadugu	Jammalamadugu	K. Sirigepalli	119	782	0	0	780	99.7
8	Jammalamadugu	Jammalamadugu	Devagudi	70	920	0	0	917	99.7
9	Jammalamadugu	Jammalamadugu	Peddandlur	118	822	0	0	818	99.5
10	Jammalamadugu	Jammalamadugu	Jammalamadugu	73	398	0	0	396	99.5
11	Jammalamadugu	Jammalamadugu	P.Sugumanchipalle	72	391	0	0	389	99.5
12	Mydukur	Khajipet	Khajipet	144	776	0	0	772	99.5
13	Punganur	Sadam	Yarrathivaripalle	166	640	0	0	635	99.2
14	Jammalamadugu	Jammalamadugu	Goriganur	76	695	0	0	685	98.6
15	Kamalapuram	Kamalapuram	Kokatam	3	445	0	0	437	98.2

the data available with the Election Commission of India:

Please note that the data provided above is not full and the complete list can be procured from the Election Commission of India website.

Conclusions V

The above table & information throws open a very important issue of Manipulation of Electronic Voting Machine. **The data definitely suggests that the Electronic Voting Machines used in the election in the above-mentioned polling booths have been manipulated.** And the only way the data recorded can be verified is with the printout of the entire votes recorded in the Electronic Voting Machine and cross verifying it with the citizen who actually voted.

Few Facts to Mention VI

The following tables gives a complete picture of the actual number of votes polled to that of the votes counted by the Electronic Voting Machine in the BHANDARA GONDIA Constituency for LOKSABHA Elections 2009.

11- BHANDARA GONDIA LOKSABHA				
Difference between the actual polled votes to that of the EVM counted votes				
LAC	Total Voters	Total Votes Polled	Votes Counted on EVM	DIFFERENCE
60-TUMSAR	251813	177786	177116	670
61-BHANDARA	294139	201173	201171	2
62-SAKOLI	265588	198450	198343	107
63-ARJUNI/MORGAON	199932	154757	155037	280
64-TIRODA	195340	141411	141299	112
65-GONDI	241090	155496	155698	202
TOTAL	1447902	1029073	1028664	1373

Conclusions VI

This is another fact that solidifies the ground for stating more sincerely that the Electronic Voting Machines have malfunctioned. These incidents signify a fact that there were not efficient methodologies adopted by the manufacturer of the Electronic Voting Machines to ensure the stability of EVM. **This is a clear indication of Electronic Voting Machine being unstable & also not being fail Safe**. If this is true how can Election Commission use such unstable & not fail safe Electronic Voting machines to conduct Free & Fair Elections?

Few Facts to Mention VII

The Elections that were conducted on 16-04-2009 to Vizianagaram Parliamentary Constituency and to Nellimarla Assembly Constituency which is a segment of Vizianagaram Parliamentary Constituency during the General elections - 2009. The particulars of the votes polled in all polling booths in Rellivalasa village to Parliament & Assembly elections are as follows:

Voting pattern parliament in Rellivalasa village of Vizianagaram **Parliamentary** Constituency Elections – 2009

Booth No.	Village	TDP	BSP	INC	BJP	PRP	Pyramid Party	Lok Satta	BSSP	Indpt	Total polled votes
70	Rellivalasa	320	06	140	08	57	04	01	14	09	559
71	Do	289	14	169	16	50	09	07	08	07	569
72	Do	313	10	223	14	90	05	07	27	12	701
73	**Do**	**133**	**07**	**11**	**319**	**71**	07	02	03	03	556
74	Do	369	10	288	21	68	11	07	24	15	813

Voting pattern assembly in Rellivalasa village of Nellimarla **Assembly** Constituency Elections in 2009

P.S.No.	INC	BJP	BSP	TDP	PRP	Pyramid Party of India	LokSatta	IND-I	IND-II	IND-III	IND-IV	Total Polled votes
70	129	7	5	332	79	4	2	0	1	0	0	559
71	170	10	8	308	41	9	6	1	4	4	8	569
72	227	23	16	326	77	9	3	3	4	6	6	700
73	**332**	**3**	**115**	**10**	**71**	4	3	15	3	0	0	556
74	276	31	8	370	91	7	6	2	7	6	11	815

Understanding the Patterns

Mr. Pathivada Narayanaswamy Naidu, candidate nominated by Telugu Desam Party, S/o Late Papunaidu, Indian, aged 70 years, secured only 10 votes in polling booth no. 73 situated in Rellivalasa village which is his birth and native place. The voting pattern when compared with the Parliamentary Elections and the Assembly Elections reveals sea of difference in respect of the votes polled to various political parties. As seen from the fact, there were no polling agents to Bharathiya Janata Party and Bahujana Samaj Party and there are no voters in the village also. But 319 votes polled to the Bharathiya Janata Parthy in Parliamentary Elections whereas only 3 votes polled to Bharathiya Janata Party in Assembly Elections.

The elections were conducted on 16-04-2009 itself for both the Parliamentary as well as Assembly constituencies. The electronic voting machines for both the Parliamentary and Assembly Constituencies were placed in the same room in each polling station. Every voter has option to exercise two votes at a time i.e. one vote for Parliament and one vote for Assembly. The elections were conducted basing on one voter's list. **More than 400 voters categorically stated and informed Mr. Pathivada Narayanaswamy Naidu that they have voted in his favour**. After declaration of the results, Mr. Pathivada Narayanaswamy Naidu came to know that the votes exercised by the voters in Rellivalasa village have not been recorded by the Electronic Voting Machine accurately to which candidate they voted by the voters.

On the face of it, the votes polled in favour of the Telugu Desam Party in Polling Station No. 73 of Rellivalasa village clearly established that the votes cast in favour of Telugu Desam Party must not have been recorded by the Electronic Voting Machine. In fact, the entire Rellivalasa village is strong hold for Telugu Desam Party. But the results are totally different. It shows that there was a defect in Electronic Voting Machines. Due to the defect in Electronic Voting Machines, the result in respect of the Nellimarla Assembly Constituency is materially affected and the petitioner lost the Election.

Conclusion VII

Electronic Voting machines were manipulated and the source code / software programme inside the Chip should have been swapped and the manipulated chips can vary / alter the results. **This is a very**

clear indication of chip getting swapped and Electronic Voting Machines manipulated to ensure results favor a particular candidate.

Further the point that needs to be seriuolsy look upon is that there were around **400 Voters** who have **categorically stated and informed Mr. Pathivada Narayanaswamy Naidu that they have voted in his favour.**

Few Facts to Mention VIII – In MP

Further there were similar incidents at Bhopal, in Madhya Pradesh. The gist of the happenings is that there were single digit votes counted on the Electronic Voting Machine in Mr. Shailendra Pradhan, **11 voters from booth no. 32 under Bhopal south-west constituency (no. 152) have solemnly affirmed under oath vide duly notarized affidavits that each of them voted in assembly elections held in 2008 for Mr. Shailendra Pradhan, who was a candidate in the said elections whereas only 3 Votes were counted in the Electronic Voting Machine.**

Remedies Proposed

Verification Tool

An open standard Verification tool can be developed, to verify the authenticity of the code inside the EVM's. All parties may buy and give to the agents to verify before or after the mock poll process, as the tool is developed by various vendors using open standards it cannot be manipulated by any Trojan.

Addition of Printer

Voter Verified Paper Audit Trail (VVPAT) or Verified Paper Record (VPR) is intended as an independent verification system for voting machines designed to allow voters to verify that their vote was cast correctly, to detect possible election fraud or malfunction, and to provide a means to audit the stored electronic results. A Printer added to the EVM can give a printout of every vote to the voter and then he / she can verify whether the vote was casted properly, and also enabling a double verification system.

According to e-Governance

According to the Draft Policy on Open Standards for e-Governance issued by Government of India, Ministry of Communications & Information Technology, Department of Information Technology and effective by July 2008; an excerpt from the Draft is as mentioned below:

What is e-Governance?

A.3) e-Government (from electronic government, also known as e-gov, digital government, online government or in a certain context transformational government) refers to government's use of information technology to exchange information and services with citizens, businesses, and other arms of government. E-Government may be applied by the legislature, judiciary, or administration, in order to improve internal efficiency, the delivery of public services, or processes of democratic governance.

What GOI suggests?

5. Policy Statement on Open Standards Adoption in e-Governance

It is imperative that India as a Nation makes use of Open Standards for e-Governance. Open Standards used by India shall have the following characteristics:

5.1 Mandatory Characteristics:

5.1.1) Selected Standard should be Royalty Free for life time of the standard.

5.1.2) Selected Standard should be developed in a collaborative and consensus manner and not led by a single agency or a small closed group of interested parties

5.1.3) Selected Standard should be recursively open; They shall not use unpublished extensions

5.1.4) Selected Standard should not duplicate already existing standard unless proven superior for replacement

5.1.5) Selected Standard should make the specification documents available without any restrictions.

5.1.6) Selected Standard should not violate domestic laws

5.1.7) Selected Standard should be made available with the same capability worldwide without any discrimination such as sub-set or super-set for different regions / countries.

Is EVM not a part of e-Governance?

Election is an integral part of the processes of Democratic governance and falls into the purview of the above-mentioned police for conducting digital poll. The Electronic Voting Machine manufactured and used in the polls conducted recently is a part of digital government and according to Government of India Draft Proposal on adoption of open standards needs to fall into this category.

Now that Electronic Voting Machines neither have open standards adhered to nor do they have interoperability i.e. there cannot be a new chip from some other vendor instead of the chip used currently from RENESAS Japan replaced into the Control Unit of the Electronic Voting Machine. Further the Source Code / Software programme developed has been kept a secret instead of adopting open standard and defining the specifications for all competent developers. Even further the hardware designs have been kept secret thus eliminating the possibility of verification of the Electronic Voting Machines by neutral third party technology teams.

Government of India have released an open standard specification inviting any competent technology developer to develop SCOSTA – Smart Card Operating System for Transport Application for the purpose of issuing Driving Licenses for Drivers, Registration Cards for the Vehicles. The adoption of open standards negates proprietary ownership of any such development, as it is meant for the use of the common public, Immense Security, eliminates Vendor Lock-ins, allows Third Party / Neutral Technical team evaluation / verification Etc.,

General Information

About Trojans

A Trojan is a code that sits silently in the original software, which goes undetected and can be activated through a key code, which is known only to the developer who inserts it. Insertion of Trojans into the EVM can further go undetected all through the Mock Tests.

Masked ROM

Masked ROM cells are once programmed, are irreversible. However, they have two major shortcomings: low security and lack of field programmability. The other major problem with masked ROM is that it is programmed during wafer processing and cannot be modified afterwards. This also eliminates masked ROM as a viable choice for storing parameters or encryption keys that may require updates during the life of the end product, unless the product manufacturer is willing to incur the additional expense of redoing the chip with updated information reconfigured into a new masked ROM.

OTP – One Time Programmable Chip

A better solution is to embed one-time programmable (OTP) non-volatile memory on the processing chip. Beyond accommodating changes in data standards and decreasing the time and cost of derivative products, OTP memory can handle engineering change orders through software modifications. Product lifetime is increased, and firmware configuration during system development enhances the co-development of hardware and software.