# The Indian Electronic Voting Machine

Dinesh Sharma

EE Department
IIT Bombay, Mumbai

ASET Colloquium
March 24,2017

# The EVM used in India

While most people would have seen the ballot unit (BU) of the Indian Electronic Voting Machine (EVM), Many may not be familiar with the other components of EVM and with the process followed in the organization of an election.

Let us see a brief video which introduces the EVM and some of the processes used during the election.

# Points to stress ...

- There is **No** external connection to the EVM through wires or wire less.
- Not even power supply mains!
- The micro-controllers used in the machines are **Mask Programmed**. This means bit patterns with ‘1’s and ‘0’ are directly connected to supply or ground using metallization. This cannot be changed by any means.
- During the poll process, machines are virtually under joint custody of candidates and Election Commission of India.

# Safety Concerns

- What if the original program from the Indian PSUs had some malicious code?
- Hex code for mask programming was sent to a foreign company which manufactured these micro-controllers. What if they inserted a hidden program in the code?
- What if the government officials who have access to the machines between polls made changes to the machine?
- Many videos on the internet claim that the EVM can be hacked. How are these people able to show that the machine can be made to report wrong results?
- “Advanced Countries” like Germany and Holland have given up electronic voting. Why is India using EVMs?

# Malicious Source Code

- EVMs are manufactured by BEL and ECIL, which also produce equipment for Defence and the Indian Atomic Energy programme. These companies have strong source code audit processes to ensure that rogue routines cannot be inserted in the software.
- The source code is reviewed by an independent third party – In this case, by a Technical Experts Committee (TEC) consisting of professors from IITs and other electronics experts.
- The Technical Experts Committee not only reviews the code, but also suggests additional safety measures as we go from one EVM model to the next.

# Code Tampering by Micro-controller manufacturers

- The EVM program contains many safety features which allow one to find out if the code actually programmed into the chips has been altered.
- For example, in the BEL machines, the program includes a “challenge-response” system.
- They have a special unit called an ‘authenticator’. The authenticator sends a challenge number and an address to the EVM.
  The EVM returns a hash of this challenge number and sixteen code bytes from the given address.
- The authenticator independently computes the hash of “good code” (with the company) with the challenge number and compares it with the EVM response.
- This process can be repeated for any challenge number and for any code address.
- Any alteration of the executable code by the chip manufacturer will be caught by this system.

# Machine Tampering While in Storage

- Machines are stored for long times between polls in strong rooms.
- When the machines are taken out for a poll, a “First Level Check” or FLC is performed.
- This involves opening up the machine, followed by a visual and function check.
- This operation is performed **in the presence of representatives of all political parties.**
- Functional check includes a “mock poll” in which representatives of political parties take part and formally certify the correctness of the result.

# Two step Randomization

To remove any motivation for tampering with the machines, no one knows which machines will go where.

- After FLC, when candidate lists have been finalized, machines are allocated by randomization.
- This is a two step process: First to allocate machines to a constituency and the second to polling station.
- EVMs (CU as well as BU) are sealed with paper seals.
- These seals are made on special paper and are printed at the Nasik security press where currency notes are printed.
- Each seal carries a unique number.
- Seals are signed by representatives of the candidates.

# Storage till Poll Day

- Machines are stored in strong rooms and guarded by armed police.
- The strong room should have a single door.
- The lock put on this door requires two keys to open it. One key is in the possession of the security in-charge guarding the strong room, while the other remains with a high official not below the rank of a district magistrate.
- **All candidates put their seals on the lock.** The lock can only be opened in the presence of agents of candidates.
- FLC and randomization is done in the presence of candidates and from then on the machine is virtually in the joint custody of candidates and election officials.

# Machine Tampering on Poll Day

Can the machines be tampered after these have been distributed to poll officials for different polling booths?

- A fresh mock poll is conducted with representatives of candidates before the poll begins.
- Correct result of the mock poll is certified by the poll officials as well as representatives of the candidates.
- The machine is sealed with a fresh seal after the results of mock poll have been verified.
- This seal ensures that you begin with a clean slate for votes and the result button cannot be pressed.
- During the poll, the official has access only to the ‘Enable’ button, ‘total’ button and poll closing button.
- The ‘total button’ permits examining of the *total* number of votes cast at any time during the polling.
- Representatives of candidates are present during the entire polling exercise and keep independent count of the number of votes cast.

# Poll Closing

- At the end of the poll, the official presses the poll closing button.
- Voting cannot be enabled after this until the result has been seen and vote counts have been cleared.
- The machine has a real time clock and records the time of poll opening and poll closing.
- Poll officials have to reconcile the register entries for polling and the total number of votes in the machine.

# Machine Tampering after Poll before counting

- The machine is virtually in joint custody of the candidates and poll officials.
- Candidates representatives are allowed to follow the transport of EVMs to the storage strong room.
- The strong room can have only one access door. This is locked with two keys. One key remains with the security in charge, while the other is with an official not below the rank of a district magistrate.
- **All candidates put their seals on the lock.**
- Facilities are provided for representatives of the candidates to keep a 24 hour watch over the strong room.
- Candidate representatives are allowed to follow the transport of EVMs from the strong room to the counting location.

# Counting of votes

- Intact seals are displayed to candidates or their representatives before counting.
- These seals are now removed to permit access to the result button.
- When the result button is pressed, the machine reports the votes polled by each candidate.
- In case the display malfunctions at this stage, an auxiliary display or a printer can be attached.

# Hacking Claims

- Many videos on the internet claim that the EVM can be hacked.
- Practically all of these refer to a demonstration by Hari Prasad et al.
- This group managed to steal EVMs kept in storage. They then removed the display and replaced it with another display controlled by a bluetooth connected device.
- While the internal data of the machine was still correct, they could display any numbers by sending these through bluetooth.

# So why can it not be done in an actual poll?

- Machines are opened and checked for any alterations during FLC.
- Machines are sealed with multiple seals with unique identity numbers, recorded and signed by poll candidates. These seals are printed on special paper by the security press at Nasik and cannot be reproduced.
- Machines are guarded 24 hours by Election Commission appointed forces, as well as candidates themselves.
- In a paper published by them, Hari Prasad et al themselves admit that physical access to the machine is essential for what they displayed. Administrative procedures make access to a machine active in poll impossible.
- Even if someone gains access, they will not be able to make hardware modifications without opening up the machine, thus destroying seals which cannot be replicated and which will be examined and displayed during actual counting.

# But advanced countries like Germany and Holland have banned EVMs

It is unfortunate that this argument is never accompanied by the actual details.

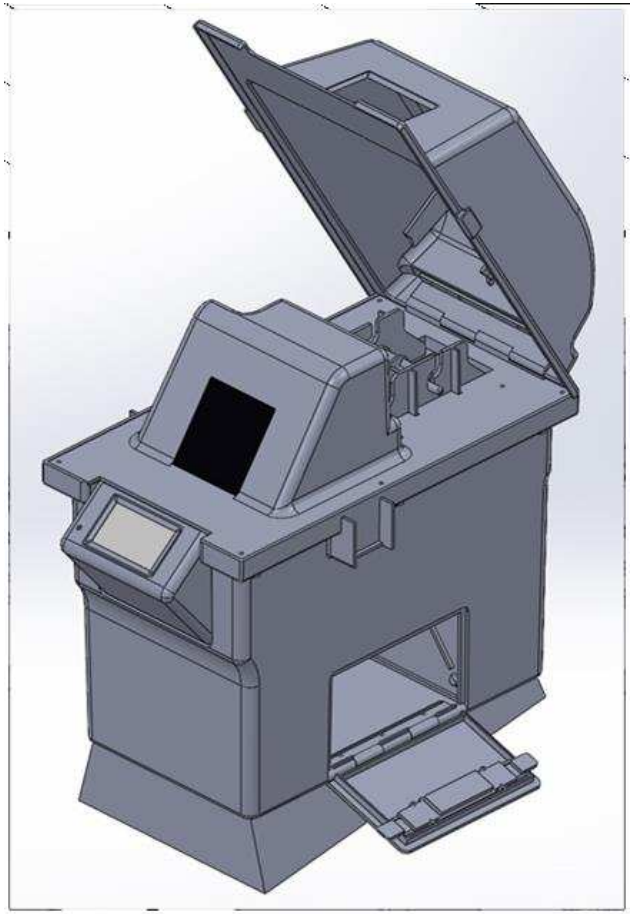
- The banned machine stored the program and data in **socketed** and reprogrammable EEPROMs!
- This machine was actually a computer which ran a program under an operating system. This OS could run any other program as well!
- This machine relied on mechanical lock and keys to control access!
- To compare this machine with the carefully designed Indian EVM along with the poll procedures is unfair.
- To suggest that if a German/Dutch machine was not up to the mark and was banned, no Indian machine can meet the required level of safety indicates a slave mentality.

# High court Observations

Five different High Courts have considered petitions that raised questions on the integrity of EVMs.

- Madras High Court: 2001
  There is no question of introducing any virus for the reason that the EVMs cannot be compared to person computers.
- Karnataka High Court: 2004
  This invention is undoubtedly a great achievement in electronic and computer technology and is a national pride.
- Other court judgments have expressed similar opinions.

# VVPAT: Voter Verifiable Printer Audit Trail



- When a voter has made a choice on the Ballot Unit, a printing unit detects it and prints a voting slip.
- The voting slip is shown to the voter through a glass window for a short time (7 seconds).
- The printed slip is then cut and falls into a secure ballot box.
- At the end of the poll, the slips in the ballot box are sealed and kept for counting.

# VVPAT: A Retro-fit

- VVPAT has been added to the EVM long after the original EVM was designed and manufactured.
- The CU and BU are mask programmed and nothing can be changed in their design.
- Lakhs of these machines have been made and represent an investment of hundreds of Crores!
- A way has to be found to add VVPAT as a retro-fit without any change in the hardware/software of the original machines.

# Communication protocol between BU and CU

- The CU and BU communicate through a serial interface (RS 422).
- The CU acts as a master and polls the BU at regular intervals to ask if a choice has been made.
- Till the voter decides on a candidate, the BU keeps reporting that no choice has been made.
- When the voter makes the choice, The BU returns the choice to the CU.
- The CU adds this vote to the chosen candidate and waits till the next authenticated voter shows up and the enable button is pressed.

# Connecting VVPAT in Eavesdropping Mode

- CU and BU communicate using RS-422.
- We could connect the VVPAT such that it eavesdrops on the communication.
- When the BU communicates a vote choice to the CU, VVPAT can capture the candidate number.
- Graphics for the slips to be printed (for all candidates) are pre-loaded in VVPAT.
- The printer prints the slip corresponding to the selected candidate, shows it to the voter, cuts it and waits for the next vote.
- It can be assumed that this operation is completed well ahead of the time that the next voter comes in.

# What If The Printer Has An Error?

What happens if the printer has an error – say a paper jam or low battery?

- The vote has already been registered in the CU but the slip cannot be printed.
- There will be a mismatch in slip count and CU count.
- Notice that the **CU count will be correct**, while the **VVPAT count will be incorrect!**
- But the purpose of VVPAT is to monitor the correct operation of CU/BU!

$\rightarrow$ **Eavesdropping mode is not suitable.**

# Relay connection


- We can connect the VVPAT as a relay station.
- It pretends to be a BU to the CU and captures messages meant for the BU.
- To the BU, the VVPAT pretends to be the CU.
- It relays the message to the BU as if it was coming from the CU.
- It captures the response from from the BU. If the BU does not have a choice to report, it relays this message back to CU.
- If the BU reports that a choice has been made, it captures the choice, but reports to the CU that a choice has **not** been made yet!

# Relay connection


- If the BU reports that a choice has been made, it captures the choice, but reports to the CU that a choice has **not** been made yet!
- It start printing the voter slip. Till the printing is complete, it keeps pretending to the CU that a choice has not been made yet.
- Only on successful printing of the slip, it reports the choice to the CU, which then adds the vote to the chosen candidates.
- Now if an error occurs during printing, the polling is stopped and a new machine is connected.
- The voter is asked to vote again on the new machine. Now the two tallies will match and both will be correct.

# VVPAT sensors

VVPAT is a printer with electro-mechanical systems (paper movement) and electro-thermal system (for thermal printer head).

Obviously, this system will have lower reliability compared to the EVM itself, which is an all electronic system.

However, we have to use this less reliable system to verify the more reliable system!

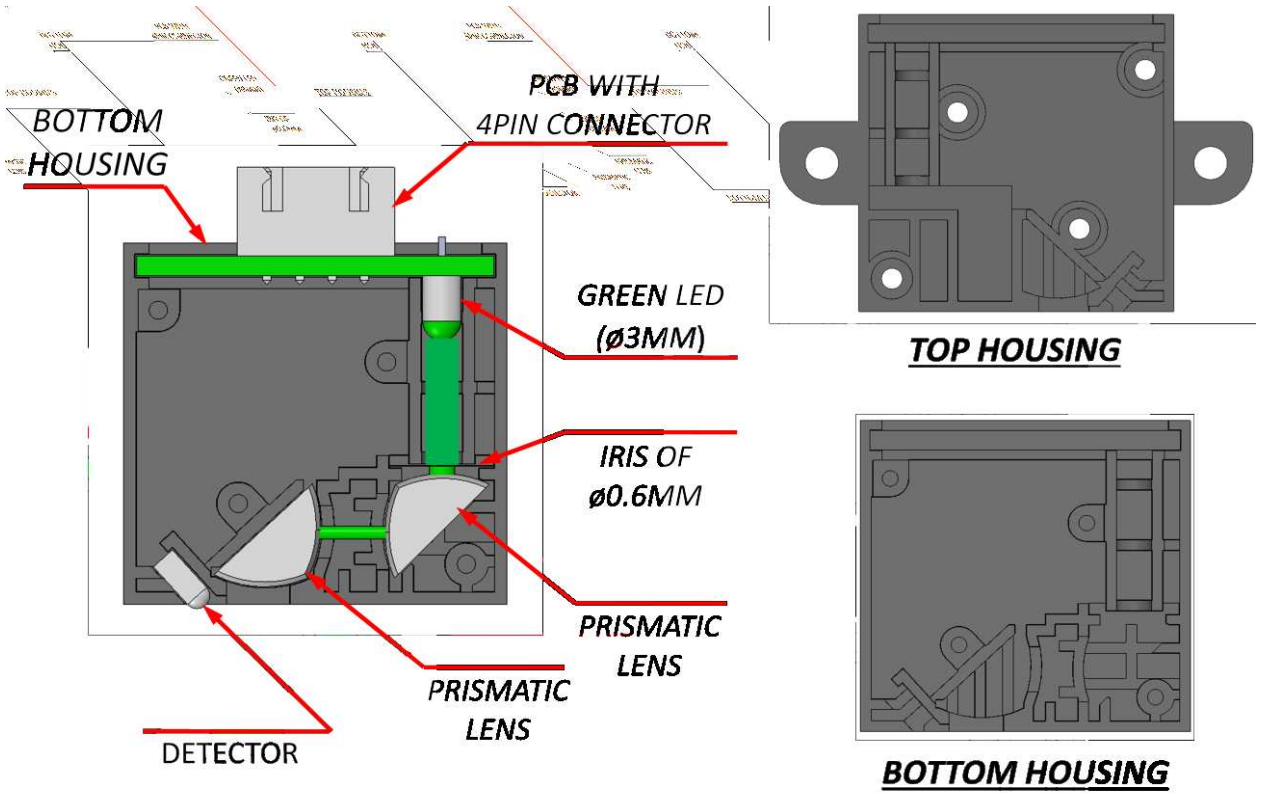
We need to enhance the poll time reliability of VVPAT to the extent possible. Several sensors have been added to the basic design to signal various possible printer failures.

# VVPAT sensors

1. A **Contrast Sensor** determines (ahead of printing the voter slip) if the current printing contrast is adequate or not.
2. A **Length Sensor** determines if the paper has any slippage.
3. A **Deplete Sensor** ensures that there is sufficient paper in the paper roll.
4. A **Drop Sensor** determines that the slip has been cut and has fallen into the ballot box before the next voter comes in.

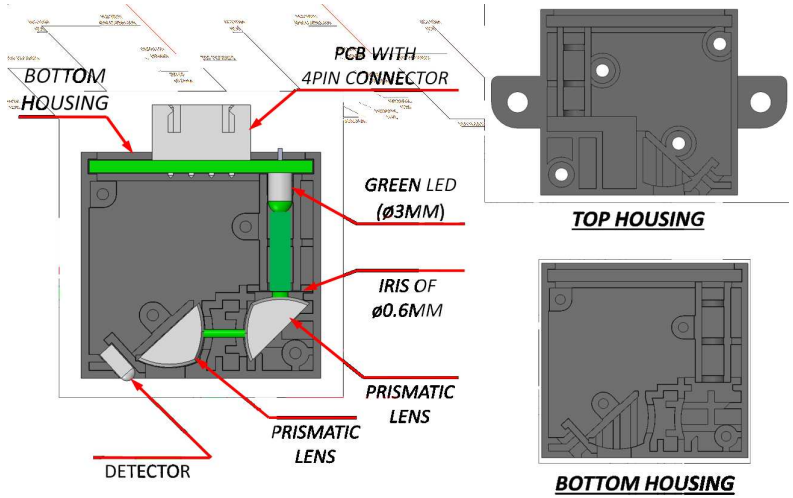
All these sensors were designed specifically for the VVPAT.

# contrast sensor



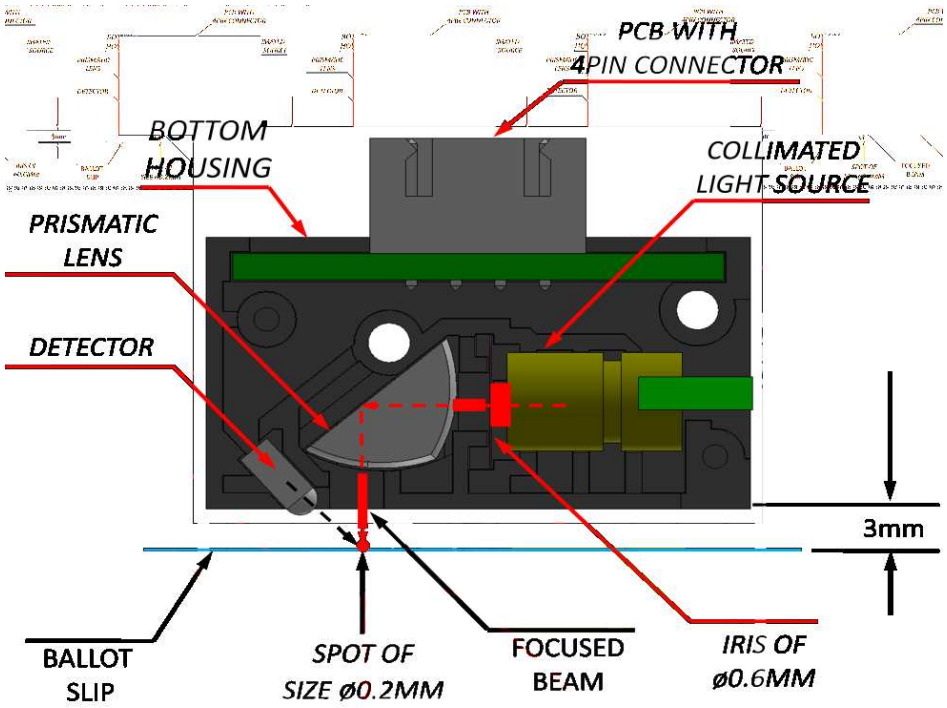

The sensor uses a prismatic lens to collimate and another prismatic lens to focus the light from a green LED to a fine spot.

# contrast sensor



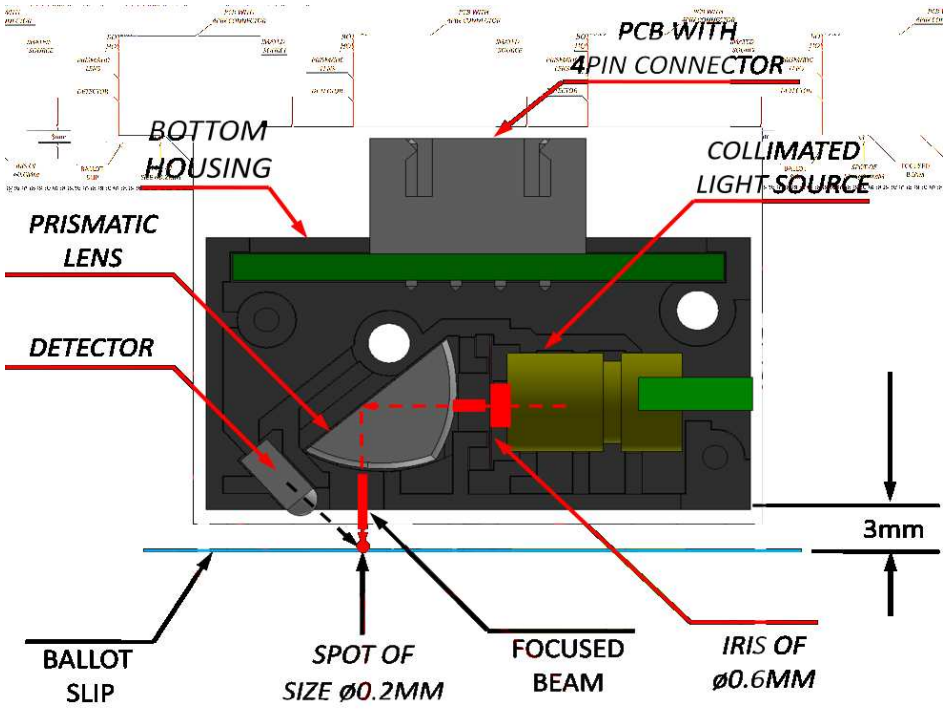

- VVPAT prints a black spot and measures the reflected light intensity from the black spot and from white region using phase sensitive detection.
- The ratio of these intensities gives the contrast.
- Green light is in the centre of visible range and gives a better measure of the contrast perceived by the human eye.

# Length sensor



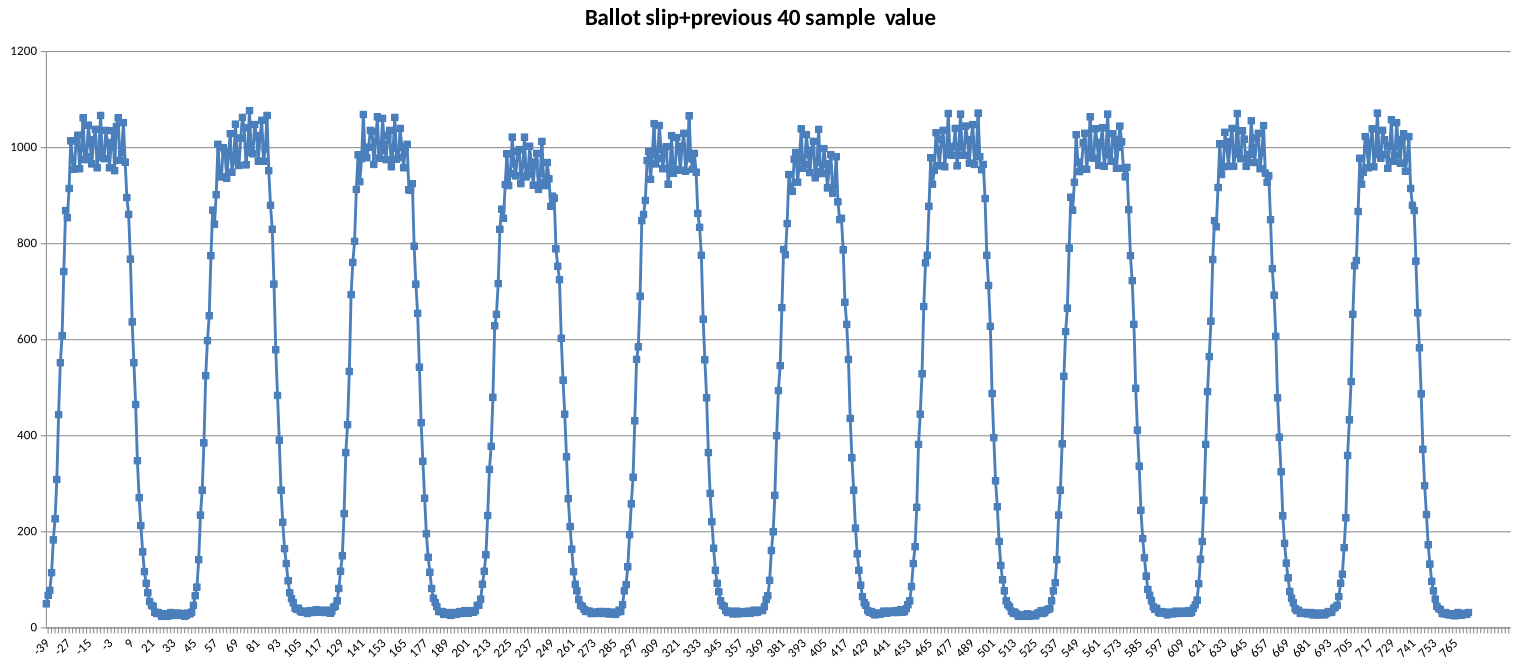

- The back of the thermal paper has fine strips with 1 mm pitch.
- The length sensor uses a red laser, so there is no need to collimate. A single prismatic lens is used to focus the light to a fine spot.

# Length sensor




As the paper moves, the detector output from the moving black and white strips is measured using phase sensitive detection.

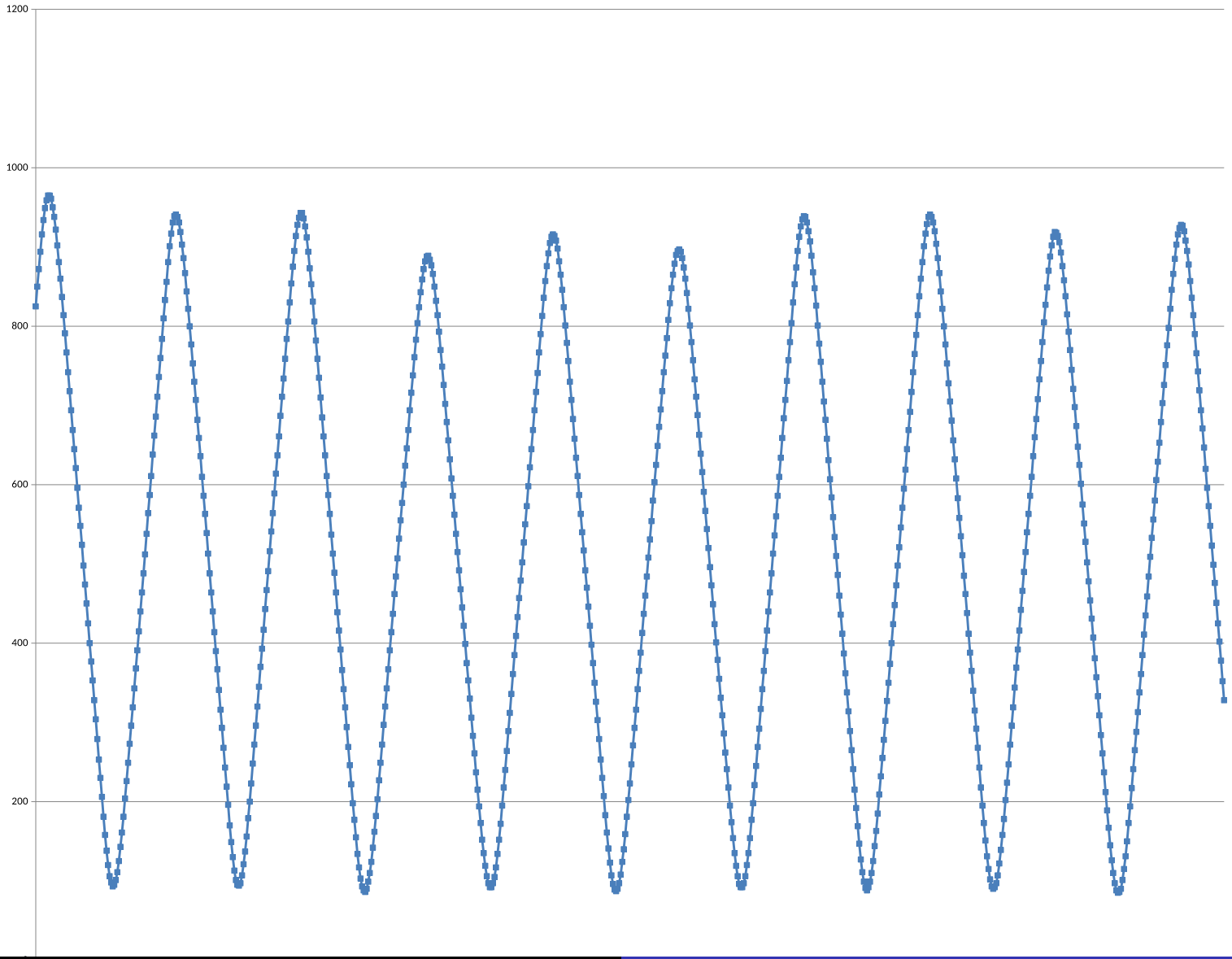
# Length sensor



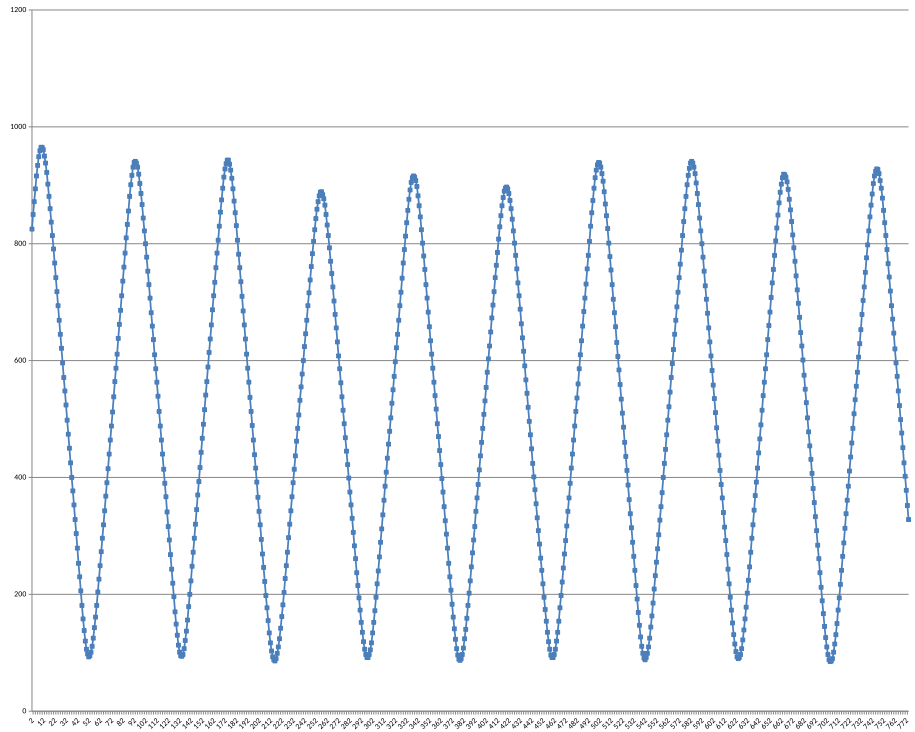

The raw data has substantial ripple at the chopping frequency used for phase sensitive detection.

# Length sensor

The ripple can be removed by taking a moving average.

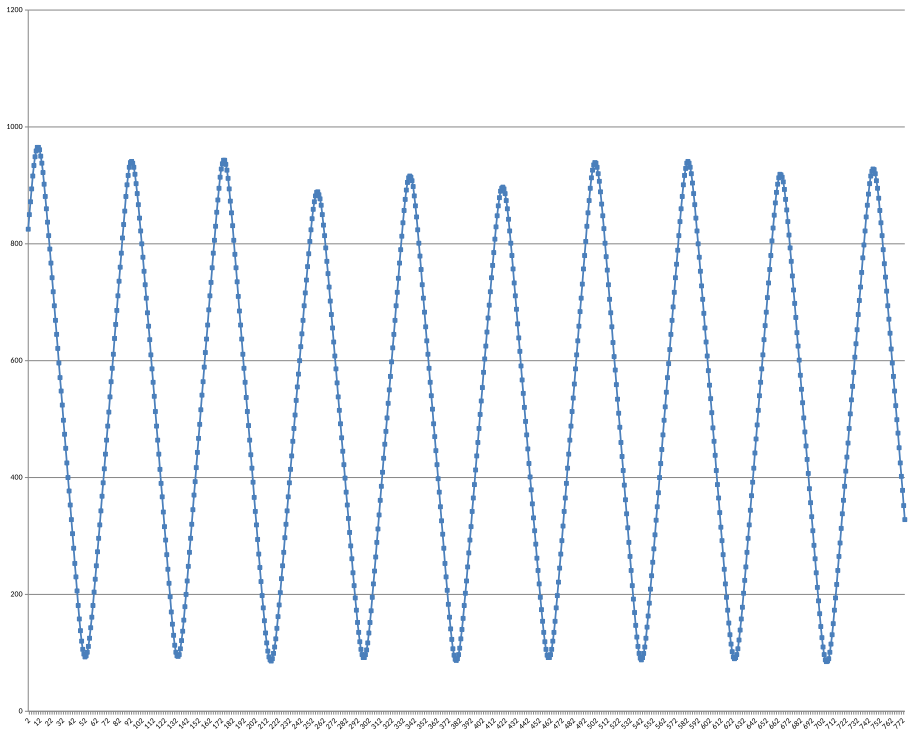


# Length sensor




- Moving average integrates the square shaped data to triangles.
- This makes it easy to locate the peaks and troughs.
- Peaks and troughs denote the edges of white and black strips at the back of the thermal paper.

# Length sensor




Counting the number of peaks and troughs, one can determine the extent of actual paper movement.

- By comparing it to the expected paper movement based on stepper motor step count, one can determine if the paper has slipped.
- (If the paper is slipping, it will take more motor steps to cover a given number of strips - *i.e.* peaks and troughs).

# Depletion Sensor

- Near the end of the paper roll, black and white strips appear at the back of the paper in the center to signal that the paper is about to end.
- The deplete sensor is identical in design to the length sensor.
- It detects these strips and generates a warning that the paper roll needs to be replaced after about 10 to 15 votes.

# Fall Sensor

- This is a simple transmissive sensor.
- If the slip has not been cut and has not fallen, the paper blocks the light beam.
- If the slip has been successfully cut and has fallen into the ballot box, the beam goes through to the detector placed at the other side of the paper.

# Future Designs

- Less dependence on humans for FLC etc. through the use of power on self test processes.
- Authentication through PKI certificate exchange and challenge-response.
- Ability to dump the code to check that code has not been changed.
- Challenge-response to check the running code through hash of externally chosen addresses which can examine code, data as well as stack segments.
- Inter-operability between BEL and ECIL machines.

# Thank You