ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 1, January 2018

Anomaly Detection Method for Electronic Voting Machine

[1] Nanda Kumar T, [2] Chiranjeevi D, [3] Sandeep B
[1][2][3] Central Research Laboratory Bharat Electronics Bangalore-560013

Abstract: **- A method for detecting electrical anomaly in circuit of interest is proposed and implemented. This method describes the use of FPGA and current sense amplifiers for real time monitoring of electrical circuits in EVM. The FPGA uses ADC and multiplexer to poll the circuit currents in round robin method. The diagnostics data recorded in used to assess the health of the unit as a whole. Necessary action is taken if any anomaly is detected. The present work is related to detect the anomaly in the functioning of an electrical circuit in Electronic Voting Machines 'units. Diagnostics is required in EVM to ensure fail proof and tamper proof voting process.**

Key words: **- Electronic Voting Machine, Electrical anomaly, FPGA based diagnostics.**

I. INTRODUCTION

Electronic Voting Machine (EVM BEL M3) has been designed to support any electoral process by providing a fast and easy mechanism to cast, validate and count the votes in an electronically secure & transparent manner. The Electronic Voting Machine or EVM, as it is popularly known, consists of the three basic units, namely

- Control Unit (CU)
- Ballot Unit (BU) - up to 24 nos.
- Voter Verifiable Paper Audit Trail (VVPAT)

that are supported by the following important Accessories:

- Printer and Auxiliary Display Unit (PADU)
- Voter Verification Unit (VVU)
- First Level Check Unit (FLCU)
- Independent Code Verification Unit (ICVU)
- Totalizer Unit (TU)

The Control Unit and the Ballot Unit are the basic and essential units that are necessary for voting. The VVPAT prints the corresponding candidate name and symbol, which can be viewed and verified by the voter. Figure 1 shows the main units of EVM BEL M3.

Earlier EVMs used only microcontroller and peripheral driver ICs for the operation in all the units of EVM. To implement diagnostics, to reduce the load on microcontroller and for reducing the cost of the units, an FPGA has been added between the peripherals of the units and the microcontroller. Each basic unit is divided into two sub- units referred to as Secure Board and Non-Secure Board. A microcontroller sits on the secure board and acts as Master Controller. All communications to and from the control unit is handled by the secure board. The secure board is named as such as it has tamper proof security implemented in hardware as well as in software level. The non-secure board has fewer security implementations compared to the secure board. On the non-secure board, an FPGA is present which acts as a slave. The FPGA functions as the controller for the peripheral operations. The non-secure board has many sensors implemented in it to perform self diagnostics of the circuits and peripherals of interest. Figure 2 shows the block diagram of connectivity of secure and non-secure board.

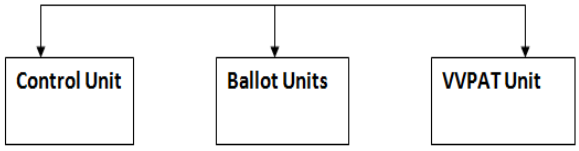

Fig 1. Main units of EVM BEL M3

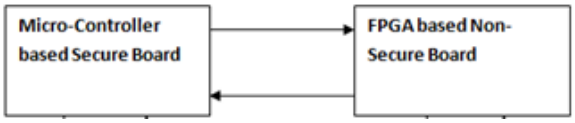

Fig 2. Block Diagram of Board Connectivity in EVM

Most of the Peripheral drivers are implemented in the FPGA, eliminating the need for their driver IC. The FPGA acts as a slave to the microcontroller and executes the commands received from the microcontroller. Figure 4 gives the block diagram of the various components present on the

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 1, January 2018

non secure board. The Entity 1 to N in figure 4 can be any peripheral like sensors, printer, keyboard, display unit and other units that needs control signals for operation. The non-secure board has many sensors implemented on it to perform self diagnostics. Figure 3 shows the general flow of command between the secure and non secure board and when the diagnostics is performed in the EVM.

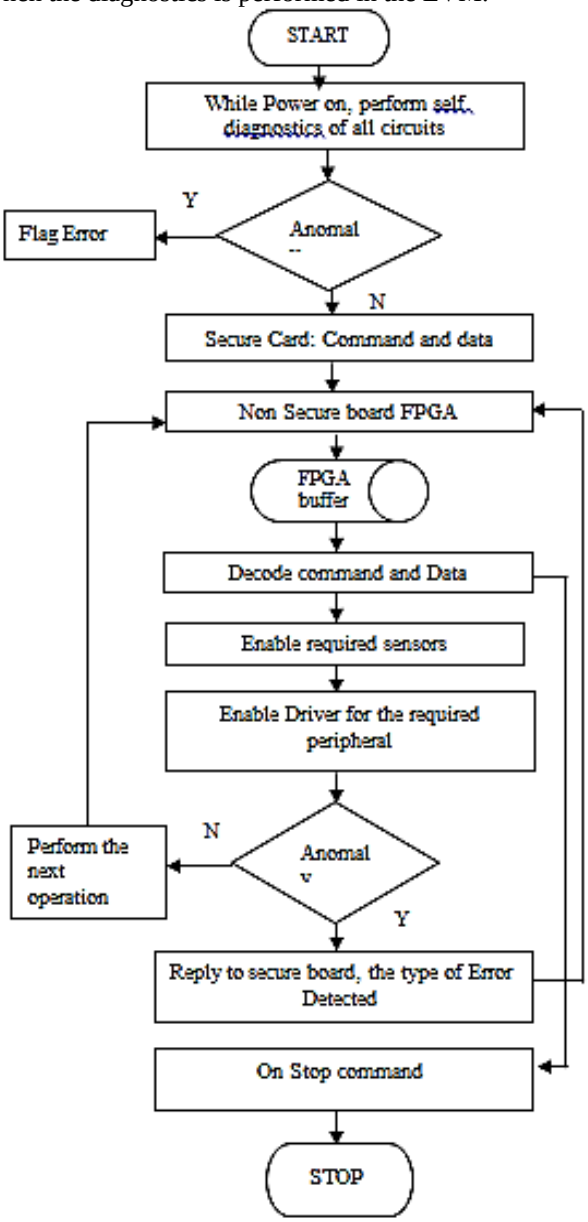

Fig 3. Flow chart of Printer Algorithm

For efficient and tamper proof operation of the EVM units all the electrical and peripherals are monitored continuously.

II. ANOMALY DETECTION

FPGA has dedicated I/O pins for diagnostics data. For every component we need to monitor, the power to that component is supplied through a low valued resistor connected in series to the feed from power supply circuitry. The voltage drop across the resistor is fed as differential voltage to the inputs of the current sense amplifier as shown in figure 5. The amplifier generates an equivalent amplified voltage as output for the given drop across the resistor. The generated voltage is then passed to an analog multiplexer. The signal select-lines of the multiplexer are controlled by the FPGA. The output of the multiplexer is connected to a multichannel ADC which is driven by the FPGA. The output of ADC is fed to the FPGA. The FPGA stores the value and performs necessary comparisons to check if the component is functioning as required or not. On standby the FPGA checks the components functionality in a round robin fashion. Based on the operation being performed the FPGA controls the multiplexer and ADC to get the specific values.

The current values are measured and checked if they are within the operational limits. Each component under test has two limits to compare with, one limit corresponds when the circuit is operational and the other corresponds to when the circuit is disabled or is in standby.

When a command is received from the controller, the FPGA enables the respective circuits and monitors the operation. If any anomaly is detected, then the type of anomaly along with read values is sent as a response to the controller. The controller takes the decision as to continue with the process or stop further processes.

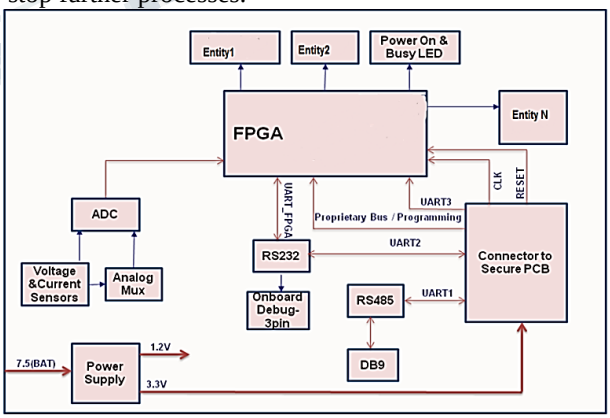

Fig 4. Block Diagram of Anomaly Detection setup in EVM

III. POWER SUPPLY CIRCUITRY

The non secure board receives power from the battery pack in the range of 5 to 8V (7.5V typ.) and is converted into 3.3V regulated output. From this 3.3V bus other voltages of 1.2V, 2.5V and 3.0V are generated for powering the rest of the circuitry. The 3.3V output also powers the Secure PCB.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 5, Issue 1, January 2018

The converters used are switching power modules for 3.3V and 1.2V operating at high switching frequencies, while the 2.5V and 3.0V supplies are generated using linear regulators. Each module is connected with suitable capacitors, at input and output pins, as per the manufacturer recommendation for the respective module to meet ripple and regulation requirements.

IV. CURRENT SENSE AMPLIFIER

Current Amplifier from M/s Texas Instruments, make, INA210 with a gain of 200V/V is used for current measurements. Current sensor resistor is connected in series between the power supply and the circuit under test. When the circuit is in ideal mode a certain amount of current is consumed, the current flow causes a voltage drop across the resistor. The value of resistor is usually very low to reduce excessive drop. The drop across the resistor is given as a differential voltage to the inputs of the Current Sense Amplifier as shown in figure 5. Since the equivalent voltage for the sensed current is low in value to be detected by the circuits at the output of CSA, we use high gain CSA. The CSA output voltage is fed into one of the inputs of the analog multiplexer. The multiplexer has much number of CSA's connected at its inputs which are connected to the other circuits and peripherals under test. The output of the multiplexer is sampled using ADC. The ADC's output is read and stored by the FPGA. The FPGA monitors the current consumed by the circuit while idle and while the circuit is operational. The current values are compared with pre-calculated value and decision is taken if the circuit is operating within requirements.

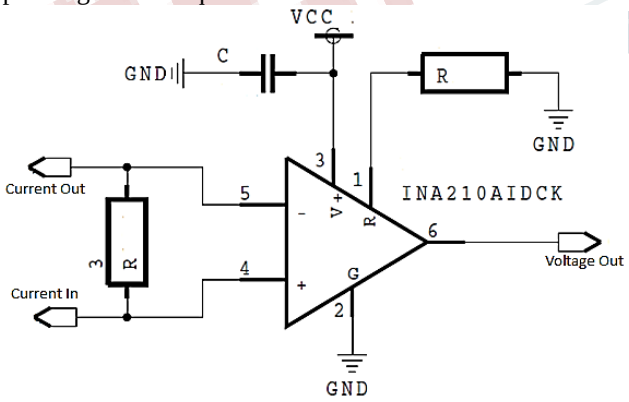

Fig 5. CSA configuration of Anomaly Detection

V. ADC

Four channel ADC; ADC124S101 from M/s Texas Instruments is used. ADC is interfaced to FPGA through SPI interface. The ADC samples the data in the channel selected by the ADC controller. The 12 Bit serial output of ADC is converted to parallel data and is sent to the FPGA glue logic. The controller for ADC is implemented in the FPGA. As the ADC is having only four channels, required number of 8-channel Analog multiplexers, SN74LV4051a from M/s Texas Instruments, is used for monitoring all the voltage and current signals. Select signals and output enable signals of the multiplexer are controlled from FPGA. Based on the command, the FGPA samples the output of ADC by activating the corresponding channel and select lines of the multiplexer. Necessary processing in done on the sampled data and the status of operation is reported to the controller.

VI. DIAGNOSTIC ALGORITHM

On initial power up, the controller initiates an self diagnostic operation. During self diagnostics, all the peripherals and critical circuits are checked for operational