Manipulation of Electronic Devices and Data in Dispensing Pumps

Nagamani.M, Vimal Babu. U, Ramakrishana.M, Sandeep Kumar

Abstract: The sale of fuel through electronics controlled based Dispensing units in the retail outlets are the source of manipulation. The stake holders are customers and are directly affected by the unauthorized manipulation by the petroleum product selling units. The electronic devices are more prone for changing the original encrypted data or stored data as a program. The program stored in this device can be altered unauthenticated by external device attached to the original circuit's boarders. The circuits board is build with the microcontroller based hardware that controls the outlet pipe by setting the control signal by the selling unit. This can be alter by changing the pulse which are used to modulate the information bits so that cheating the customer by alter the set control bit by deliver less or more through the dispensing unit. This research article focus on explore the possibilities to make the encryption method of control bits more robust than the present simple pulse modulation techniques.

Keywords : Microcontrollers, Software language, Memory cards, Pulsars, External devices, Dispensing Units.

I. INTRODUCTION

The petroleum products fuels like Gasoline (Motor Spirit), Diesel, Kerosene are widely used in the Internal Combustion Engines to run the vehicles, Power generation etc. The fuel for these is dispensed from the fuel dispensers situated at the retail outlets. The fuel dispensers previously used with the mechanical dispensers to deliver the fuel and subsequently changed to the electronic dispensers. In the mechanical dispenser the fuel is measured with the displacement of piston volume in the cylinder contained in the metering unit. With the recent development of sensors and incorporation of its technology in the measurement of volume, the pulsars are utilized to count the pulses. These analog signals are converted into the digital signals for display. The microcontrollers are used to program the interruptions and relay for control the volume dispensed. With the change of the program in the microcontrollers, changing the memory chips in the motherboard the delivery through the dispenser is manipulated to the benefit of the trader. The high end software languages like C/C++/JAVA are unable to detect the change in the data stored. This is ultimately causing the non detection of the external software and/or insertion of the spurious electronic devices which are causing the short delivery of the fuel to the end consumer in terms of volume. The article offered the method to make use of the large data collected by the sensors and actuators in the industry a Cloud-based architecture for Internet of Things (IoT) to improve the satisfactory working of different phases of the industry, optimize industrial process and make longer life cycle of the watched machines. Industrie 4.0 [1]. The navigation is a real-time operation where as the remote sensing is post-processing mode. The difference between the remote sensing and the navigation is described with the innovation of new sensing devices and the utilization of the enormous quantity of data gathered. Platform development is reviewed with main focus on Unmanned Aerial System (UAS) platforms and emerging new remote sensing satellite constellations. Next, an enabling technology for remote sensing, i.e., sup- porting navigation infrastructure and sensor geo-referencing, are discussed. Finally, sensors based on their spectral, spatial, and temporal characteristics are grouped and classify them by their platform deployment competencies. Better sensing and modelling our physical and social environment has always existed from the societal side. The ongoing paradigm shift in navigation has started a convergence process between the remote sensing and navigation fields [2]. 15 Medipix2-based detector devices execute a real-time measuremenst of the composition of radiation and the spectral characteristics inside the ATLAS detector during its operation [3]. Internet-based, service-oriented system employs Augmented Reality remote tele-maintenance platform technology help client and manufacturer [4]. With the help of four-channel Remote Control (RC) is tailored to control multiple DC motors and other devices on Unmanned Guided Vehicle (UGV) [5]. The uniqueness of EEG (Electroencephalography) signal can be exploited to remove some of the drawbacks of the existing systems. Secure mobile devices using Electroencephalography signals along with existing pattern-based authentication. Electroencephalography signals are modeled using HMM (Hidden Markov Model), and using a binary classifier implemented with SVM (Support Vector Machine) to verify the authenticity of a test pattern. Verification performances are measured using three popular security matrices, namely DET (Detection Error Trade off),

Manuscript published on 30 September 2019.
***Correspondence Author(s)**

Naga Mani.M, Senior Assistant Professor, School of Computer and Information Sciences, University of Hyderabad, Gachibowli, Hyderabad-India-500046,
Vimal Babu, U, Research Scholar, Mechanical Engineering, Vignan's Foundation for Science, Technology and Research (Deemed to be University), Vadlamudi, Guntur, AP-India,
Dr.Ramakrishana.M, Dean, IQAC & Professor, Mechanical Engineering, Vignan's Foundation for Science, Technology and Research (Deemed to be University), Vadlamudi, Guntur, AP-India
Sandeep Kumar, Student, School of Computer and Information Sciences, University of Hyderabad, Gachibowli, Hyderabad, India-500046,

HTER (Half Total Error Rate), and ROC (Receiver Operating Characteristic) curves. Biometric based authentication systems are usually helpful in reducing some of the susceptibility but with some limitations. For example, facial expression and finger-print guided authentication systems are prone to wax molding, copying, and photography. Speech-based authentication systems can be easily targeted by mimicking the voice. Moreover, some of these biometric information may change with time. So, a robust authentication system may be quite handy if it is less prone to such susceptibility [6]. Online VRL (virtual and remote laboratories) cannot sup- port the Java script so also complex virtual and remote laboratories can overload the device while running, hence new model which support the hardware devices. The problems faced in the use of mobile devices in running the Java/JavaScript Simulations (EjsS) identified in the use of online VRL and the remote connection of hardware with the help of JavaScript. This is a new configuration to again make use of virtual and remote laboratories which uses a Java model that runs on the server and a JavaScript Graphical user interface on the client side [8]. The patient health condition especially fever i.e., pharmaco kinetic and pharmaco dynamic analysis can be monitored with the paradigms of AmI, UC and IoT. The data torrent from devices with a 3D printer design can avoid medication errors, proper medication [9]. The remote practices for Systems Engineering and Automatic Control laboratories based on EJsS (Easy JavaScript Simulations), Node.js and Raspberry Pi. Easy JavaScript Simulations is used to create a HTML5 and JavaScript laboratory front-end that lets user parameterize and observe the condition of the systems under study from the web-browsers of their laptop or smart phone. Through GUI user parameterize the condition of the system and observe the evolution of the system signals, the servers that handle the access to, the controller application that take care of closing feedback loop over plant under observation , and connection of Graphical User Interface and controller [10]. The remote maneuver of the vehicles is done by Imaging Package for Remote Vehicle (ImPROV) using mobile net- works, time-stamped imagery, and positioning etc., has no range limitation, having the LTE coverage worldwide, prop up multiple cameras, long-range encrypted communication, live streaming. [11]. The movement to the disabled persons through Tele rehabilitation (TR), a remote wheelchair selection (RWS) is an up-and-coming meadow that harmonizes the current in- person consideration for choose a suitable wheeled mobility and seating device. PMD alternative generation algorithms put into practice support on PMD terms and needs counting HCPCS-powered mobility device codes [12]. The precise properties of IXs raise an appropriate method for studying fundamental properties of cold bosons and for the advance of signal processing devices based on excitons [13]. The use of the Ethernet, VPN (Virtual Private Network) for remote watch, programming of PLC systems and using remote USB interface for industrial devices programming is presented in the paper. International Journal of Information Management 34 (2014) 336343 Management and Real time exploration of huge medical volumetric data sets on small mobile devices can be done with the help of approach Tomasz Hachaj. [15]. The only one of its kind field Robodrom constructed to study the remote and networked control algorithms through online game with wireless network , keeping the constraints of bandwidth limit, delay jitter, and packet dropouts. The IR remotes can be used for very low range of the order of 10 m and the RF based remote controls for the range of less than thousand meters with a limitation not to use in under- sea, automated driving or online fire fighting [16]. The data exchanged/interacted among Internet of Things (IoT) robustly so also the hardware part of the devices [17]. The universal remote (Micro controller Chip PIC16CX) to be in command of all home appliances in a house using radio frequency remote (act as repeater) control system, and sensors built- in superficially to the devices. This system can be enhanced by means of the alarm. Two way handshake communication systems is used to detect the failure system [18]. The biometric system is believed to be authenticated system to identify the person. Even this biometric system is not tamper proof. This system can be secured from assail from a smart card, a text password, and a biometric identity. The Remote client validation system is engaged such as ATMs (Automated Teller Machines), WSNs (Wireless Sensor Net- works) and TMIS (Telecare Medicine Information Systems). [19]. Physically disabled persons or senior citizens who are not able to move from one place to another can be moved with the help of electric-powered wheelchair with the remote control by using mobile devices. Some time it can be fitted with a camera to avoid collisions [21]. VRL developers a latest composition to use again VRLs with the use of a Java model that runs on server and aJava script GUI on the client device [22].

II. RESULTS AND DISCUSSION

Each weighing or Measuring instrument which is being used in the transaction relate to the public is governed by the law in order to protect the human being to ascertain the accuracy of the machine. For this government is issuing the model approval certificate for each model of the machine. The machine shall be periodically re-verified to maintain the accuracy of the machine.
The Model approval certificate issued by the approval authority i.e., Government of India, for dispensing pumps are used for delivering the petroleum products at retail outlets shall conform to the physical characteristics, configuration and construction material written in Model Approval Certificates. The Government of India issues (represented by the Director of Legal Metrology under rule 11.1.g of Legal Metrology Model Approval Rules 2011)) such certificate to the respective machine with specific number. In practice the measuring machine shall ensure that the machine is meeting the established performance and tolerance as specified in the Schedules under the Legal Metrology (General) Rules, 2011 of India.

In order to retain the accuracy of the product to be delivered the machine parts are sealed by the statutory authorities with the equipment provided to them. The vulnerable parts of the machine and the places to be sealed are as written in Model Approval Certificates.

By the Government of India represented by the Director of Legal Metrology (Rule 11.1.g of Legal Metrology Model Approval Rules 2011) and are ensured by the enforcement agencies. It is ensured that the machine approving authority is a position to know the places of manipulation while conducting tests (Rule 7 of Legal Metrology Model Approval Rules 2011) for as stipulated by him in the model approval presented to him under rule 5.2.b of Legal Metrology Model Approval Rules 2011. Such places are affixed with mechanical seals, to prevent manipulations, some times to take up electronic sealing methods where there are cases with the use of extra peripherals Eg: remote control for altering the values. The seals are provided on the machine parts (Rule 2.20 of rules) to ensure the gauge parts, which cannot be materially protected in any other way against the regular usage and are likely to affect the measurement accuracy. There shall not be any change in the parameters influence the strength of the results of conversion, correction, and measurement, parameter particularly, through way of sealing device. Sealing also prevents access to the calibration point of the instrument. Sealing is made to protect the reliability of the machine or the weight or measure. The sealing may require when there it is prone for altered metrological characteristics of the machine caused due to replacement of parts, recalibration or mal- adjustment of the parts.

The regular parameters in determination of the results of the machine and the parts which influence the regular usage of such machine shall be protected by way of sealing. Electronic sealing can also be used in place of mechanical sealing of the device parts. It can in password form or hard key. The iterations used for accessing the parts which influence the delivery of the product through the electronic sealing be memorized which shall be stored for a minimum of 2 years and the record should include date and the characteristic element which identify authorized person who make intervention, traceability of intervention, deletion of information must also be reflected.

If tampering of the sealing wire or seal can not get detected, it is similar as non-sealing. Only twisted wire with square lead plugs are recommended for mechanical sealing to ensure firm fixing. These seals if tampered can easily be detected. The square lead plugs should be pressed such that the twisted wire cannot move in the hole provided. The places and lead seals may prominently indicate in the certificate of verification.

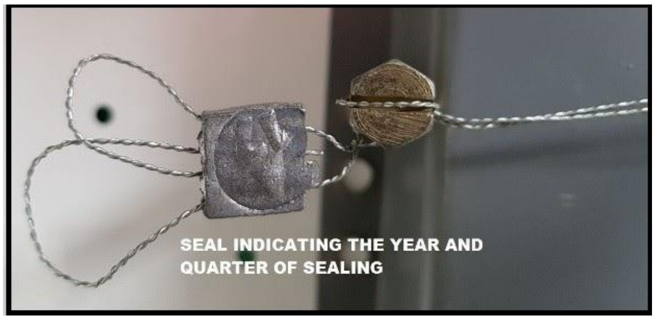


Fig. 1. Statutory Body Seal

There is no precise regulations in respect of hardware parts namely Hose pipe, Air separators, Vapour collectors, Connections to tanks, Nozzle, Interlock, Oil Seals, Display of price, which also influence the delivery of the product through the machine. The processing unit of the dispensing pump will be con- trolled with a device fabricated on the PCB to generate a supplementary passageway for the unauthentic signal transitory to the Central Processing Unit and the device can be maneuver in the course in the operator room by an on-off switch. The mother board of the dispensing machine contains the prerequisite for in command of delivery of the product with minor tolerances other which is called dip switch. Therefore it is mandatory to seal the dip switch in order to stop further access to the operator for fraudulent use of the dispensing unit.

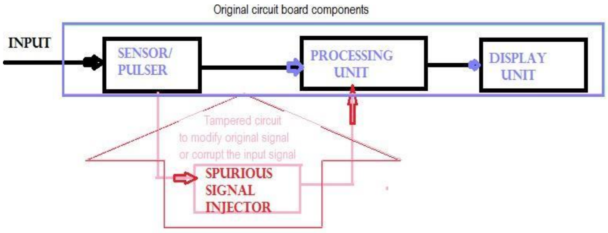

Original circuit board components
INPUT
SENSOR/
PULSER
PROCESSING
UNIT
DISPLAY
UNIT
Tampered circuit
to modify original signal
or corrupt the input signal
SPURIOUS
SIGNAL
INJECTOR

Fig. 2. Block diagram of the sending spurious signal

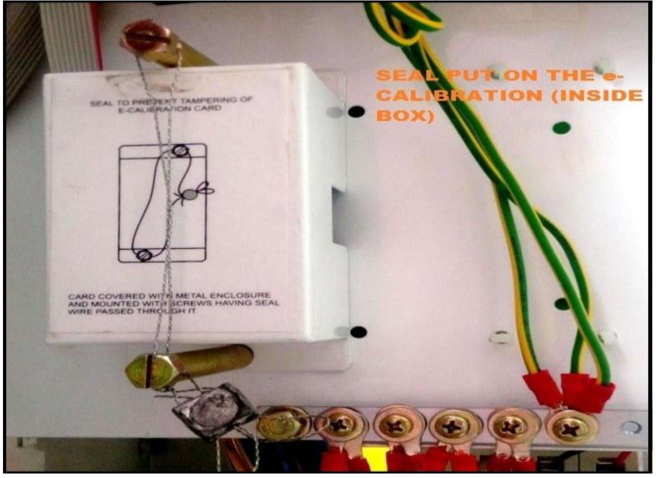

SEAL PUT ON THE e-
CALIBRATION (INSIDE
BOX)
SEAL TO PREVENT TAMPERING OF
E-CALIBRATION CARD
CARD COVERED WITH METAL ENCLOSURE
AND MOUNTED WITH SCREWS HAVING SEAL
WIRE PASSED THROUGH IT

Fig. 3. The figure shows 2 black boxes, having a Dip Switch in each one for the calibrating 2 separate nozzles.

Note:-The wiring should be followed according to Figure No.:- 3 so, that boxes can't be opened without altering verification seal and denied access to Dip Switch.

A. The OTP (one time password):

There is an innovation in the manufacture of Dispensing pumps (Petrol/Diesel pumps) make (Eg: Midco, Gilbarco make, etc.) with a facility of remote control over the delivery. This is paving the way for the fraudulent use of pumps by the private operators, for wrong delivery of petroleum products like Petrol/Diesel to the consumer. The password is directly coming as a mobile alert to the private operator instead of statutory authorities who are calibrating the accuracy of the machine.

Taking the advantage of password that is being supplied to the private person by the original equipment manufacturer, who is otherwise assigned the annual maintenance contract of the machine, is changing the characteristics of the machine architecture so also the delivery of the product through the machine. Ultimately the end consumer is being affected in getting the worth of the product contracted for and paid for. Cryptographic data shall be used in order to disable the data for unauthorized persons use. The data can be kept protected and retrieved by hash case transfer for authentication in electronic signing by using the pair key system, one secret and the other to the public. With the use of software languages like JAVA, C++/C, etc., it is very easy to detach the data of one program module from access with any other program modules. The Device-specific parameters and configuration parameters data can be identified.

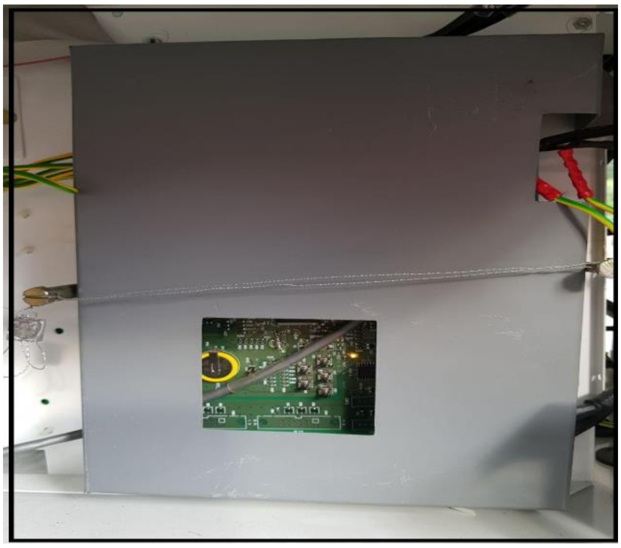
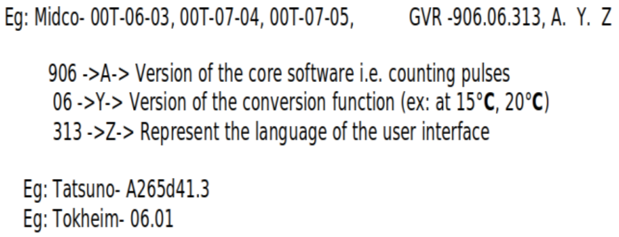


Fig. 4. The Mother board will be sealed in order to prevent the access of the Mother Board for inserting the additional devices. The opening is meant for making the display price alteration whenever there is a change in selling price of the petroleum products.

B. Sample of Software version used in Dispensing Pumps:

Software identity of the measuring instruments is called Software Version. Generally Software version contains a textual string or a number.



Eg: Midco- 00T-06-03, 00T-07-04, 00T-07-05, GVR -906.06.313, A. Y. Z

906 ->A-> Version of the core software i.e. counting pulses
06 ->Y-> Version of the conversion function (ex: at 15°C, 20°C)
313 ->Z-> Represent the language of the user interface

Eg: Tatsuno- A265d41.3
Eg: Tokheim- 06.01

Eg: Tokheim- 06.01 The failure in pulse-modulated fuel system may be identified by a built-in engines PCM (Power train Control Module). When the Power train Control Module senses longer pulse than usual pulse width, which is required to meet the directive fuel pressure level, it also stores diagnostic trouble codes in the diagnostic memory which signify that the fuel bunk is not working at the directive level. The original manufacturer of the machine shall ensure the correct identification of the software (textual string or a number, explicitly recognize the installed version in the approval certificate issued to the particular machine by the statutory authority.

III. OIML (“INTERNATIONAL ORGANIZATION OF LEGAL METROLOGY) D31 PECIFICATIONS”)

(“Organization Internationale de Metrologie Legale” is created to promote the Global Harmonization of the Legal metrology procedures and was created in the year 1955, and having headquarters at France.)

According to OIML D31-2008(E) the general requirements for software controlled measuring instruments are as follows

- The Software can’t be changed; it may happen in one situation when any hardware parts are changed.
- The identification of software (software version) should be stated in the model approval certificate.
- After any updating in legally relevant software of the measuring device, the measuring devices are not allowed to be installed for selling purposes before verification of device from Legal Metrology as discussed in Section 7.
- Software updates have to be recorded in Audit trial.
- Executable file of a software version has to be protected against modification by checksum.
- Checksum algorithm calculates checksum of the executable code.
- The checksum algorithm should be the normalized algorithm. Ex : CRC 16 Cyclic Redundancy Check

A. Check Sum:

The checksums are a sequence of letters and numbers used to check for errors in data. When data are sent from one device to another device, first some bytes of data, i.e., checksum is added to the original data and then send. On receiving data, side receiver should know the checksum for checking the originality and authenticity of the data. the most common checksum calculating algorithm is Cyclic Redundancy Check (CRC), MD5 (Message Digest Algorithm), SHA-1,SHA-2,SHA-3, 256, 512 (Secure Hashing Algorithm)

a) SHA-512 is the most authenticated checksum algorithm for calculating the checksum.
b) Checksums of some Dispensing
Units Eg: Midco 0x555BAFT
Eg: Dressewayne-
2abe Eg: Tatsuno-
2363

The electronic measuring instrument and its software shall be so manufactured that it shall be less prone to the impending for unintentional, inadvertent, or intentional misuse.

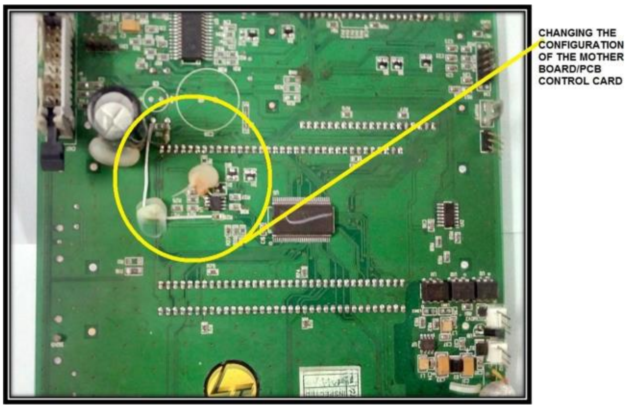

CHANGING THE CONFIGURATION OF THE MOTHER BOARD/PCB CONTROL CARD

Fig. 5. External devices are inserted in the main Mother Board for fraudulent use. The software is not detecting such external devices.

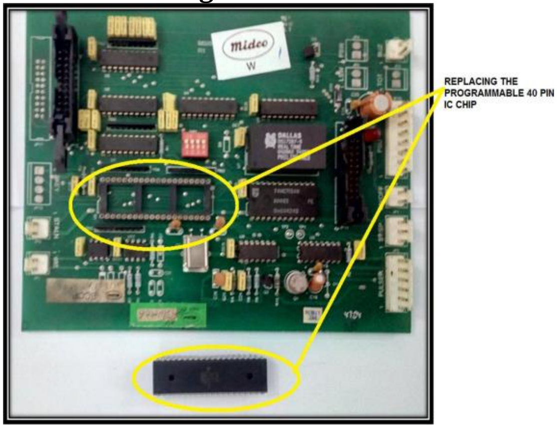


Fig. 6. Detachable Micro Controller fitted in the Motherboard. This Microcontroller can be programmed at any stage even when the instrument is sealed by the statutory authorities.

IV. Microcontrollers

A microcontroller is a tiny size computer on a single board integrated circuit. In modern days, it is but less sophisticated than a system on a chip. A SoC (system on a chip) has a microcontroller as one part. A microcontroller has programmable input/output peripherals and one or more central processing units along with memories. OTP ROM or NOR flash ferroelectric RAM is used for programmable memory onboard, Microcontrollers are mostly used for embedded applications, rather than microprocessors used in regular computer and laptop. Microcontrollers are used in implantable medical devices, automatically controlled products and accessories, such as remote controls, automobile engine control systems, power tools, office machines, appliances, toys, etc.

Microcontrollers are small and cheaper in comparison to a microprocessor. A mixed-signal microcontroller is standard, integrating analog components needed to control an embedded system. Microcontrollers are commonly used in the field of internet of things (IoT) to sense the environment and data collection.

Use of Microcontrollers is also a very economical way to implement in the real physical world.

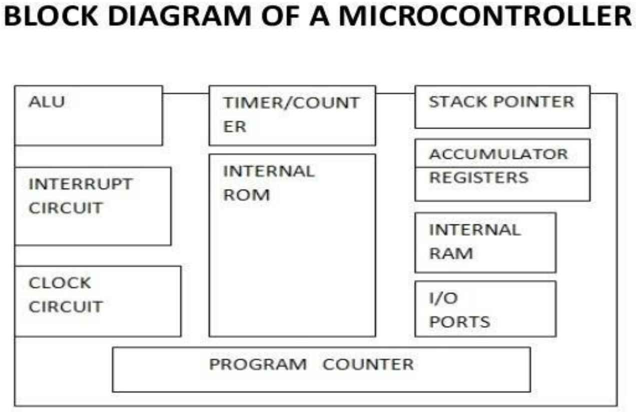


Fig. 7. Block Diagram of the Micro Controller

The Memory device of the gadget shall be isolated from the deceptive use, unauthorized adaptation, loading, or changes by substitution of the memory device. Earlier the memory device is not preserved by the statutory authorities, thus making the machine to the fraudulent use at the memory device attached to the PCB. Now the circumstances necessitate sealing the Motherboard housing clasp the memory devices shall be sealed on PCB. The circuits are manufactured in this fashion that write-protection can't be altered through short-circuit...

40 pin IC PROGRAMMED FOR ALTERING THE SOFTWARE (MIDCO MAKE , BULLET_

Fig. 8. Microcontroller used for altering the programme in MIDCO, Bullet.

40 PIN CHIP USED FOR MANIPULATING THE PROGRAMME
SEIZED FROM MIDC O MAKE (Bullet)

Fig. 9. Microcontroller used for altering the programme in MIDCO, Bullet.

The Program Counter executes the program in the addition of one instruction, and the value of the program counter can be altered at any moment, which causes a jump to a new memory location. The main Motherboard of the electronic dispensing pumps is built-in with the microcontroller, which is having the features of counting the pulses. The PC and available high- level programming are used to write a program for running the microcontroller for real environment simulation.

Here the microcontroller is so programmed for delivery of the product from the dispense that after reach of the product to the 55% or some time 65% of the liter measure the volume delivered will be correct and there on there will be the short delivery to the end-user i.e., the timer is programmed to suit the vendor. The input/output ports can modify a pin utility according to the vendor's desires. Unfortunately, the software installed in the electronic machine is not detecting such altered program in the microcontroller. This is paving the way for the fraudulent use of the machine to gain unlawful profit by the vendor.Along with mechanical sealing, technical means are used to secure measuring instruments, which have an operating system or memory for uploading operating system. If the loaded Operating System of the instrument is uninfringeable in a memory like ROM then technical sealing requirement may be less. Measuring mechanism may have sub-assemblies of doing the metrological functions and other a universal computer with the operating system. The manipulation can be restricted by easy means of cryptography. This is encryption of the data transferred between the universal computer and the sub-assembly. Here fully and cleared documented function is activated by user interface. So, that it does not facilitate fraudulent use. Here the 40 pins 89C55-Microcontroller has been manipulated to alter the bits transfer, for manipulation. Unmistakably recognized functions are allowed to be activated by the user interface, which shall be recognized in such ways that it does not help fraudulent use. The input from the user interface is redirected to a program that filters incoming commands which allow and lets past the documented ones and discards the rest of others. Device-specific parameters to be secured are stored in non-volatile memory. Though write-enable inputs of memory is inhibited or controlled by a switch, the traders are resorting to the fraudulent practice such that they are inserting the pulse generator with the remote operation to manipulate the inputs. The above figure gives the interface which is used to manipulate the inputs, and such inputs are not filtered by the program.

V. NOVEL METHODS OF FRAUDULENT PRACTICES IN DISPENSING UNITS (DU)

- By shutting down the DU, bypassing the battery wires leaving the single wire from the battery without connecting the emergency switch.
- Communication Bus (Cable) from the calibration card to the connector of the calibration card in the motherboard will be removed.
- An external plug-in device with modified K-factor was inserted into the calibration card connector of the motherboard in place of regular communication bus (Cable) from calibration card.
- In this process K-factor was cloned, manipulated and communicated to CPU/Motherboard/Control card by way of intended plug-in device.
- This process does not require either disturbing Legal Metrology Seal or any other kind of authentication to be recorded.
- Once the tampering and consequent short delivery is affected, even if external plug-in device was removed and connection of cable of original calibration card was installed, the affected short delivery continues until the DU is restarted.
- It happens because the control card requires K-factor only once when DU is started.

VI.HOW TO CRACK THIS?

a) Physical Measurement of the product delivered through the DUs. Take 5 Liter measure of the product through the DU and poured into the standard measure.

b) Take swift alert so that no person should operate emergency switch of the DU.

c) Find out any imprints of bypassing battery cable to the emergency switch and vice-versa.

d) Physical inspection of other side of the mother-board with naked eye for R201, R202, and D49 chips.

e) Normally short delivery through DUs is reversing of the totalizer or forwarding simultaneously.

f) Observe initial reading, run the DU for 20 liter, then test totalizer reading.

g) In MIDCO, Sure fill and Accufill models, if we press T-button on keypad (like emergency switch in GVR) normal condition prevails.

h) Generally manipulations in MIDCO make DUs can be done through keypad only.

i) The paper print of the sales through the MIDCO, make DU reflect the short deliveries. It is a big problem for manipulators such that they shall be are definite in assuring the keypads are not in working condition especially for the manipulated DUs. The Software protection comprises appropriate sealing by electronic, mechanical, cryptography, which make the unlawful involvement or evident.

A. The Electronic sealing

The input of meteorological parameters are identified, registered by the software and each change, augmentation can be indicated. The indicated value and the registered one is varied it can be inferred that the instrument is in an unverified state (tampered seal). The switch may be provided such that without operating the switch it is not possible to alter the specified parameters and configuration and that switch shall be sealed with the mechanical means. Without breaking the seal it is not possible to alter the parameters. The seal can be broken by the authorized persons. The retail outlets are providing smart cards include PIN as a cryptographic certificate for recognizing the person who is operating system for entering parameter menu item. Software system is capable of validating the authenticity of the PIN with certificate and then the access are recorded in the audit trail.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

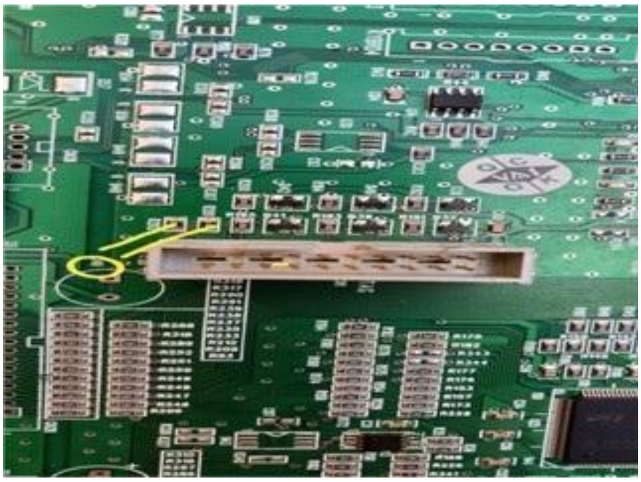


Fig. 10. Manipulated chips of R201, R202 and D49, which delivers short

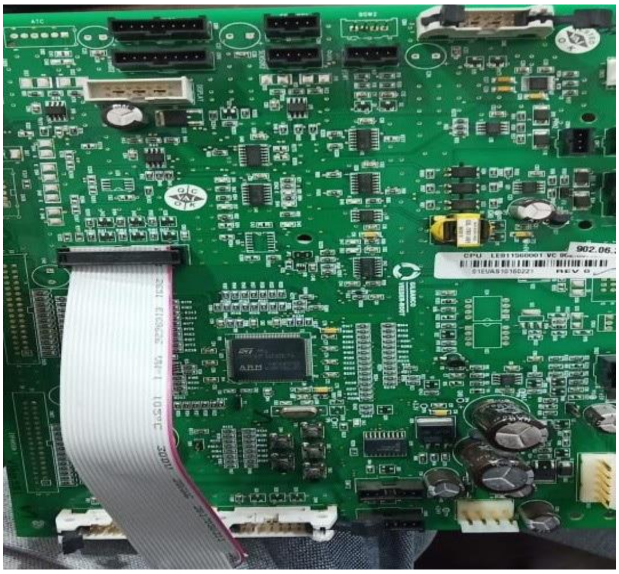


Fig. 11. Bypassing Calibration Cable; b. Chips Soldered to manipulate the circuit path

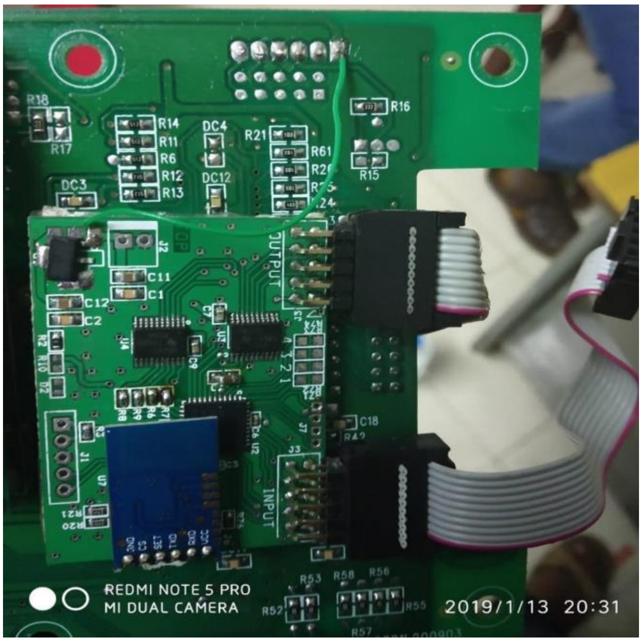


Fig. 12. Bypassing Calibration Cable; b. Chips Soldered to manipulate the circuit path

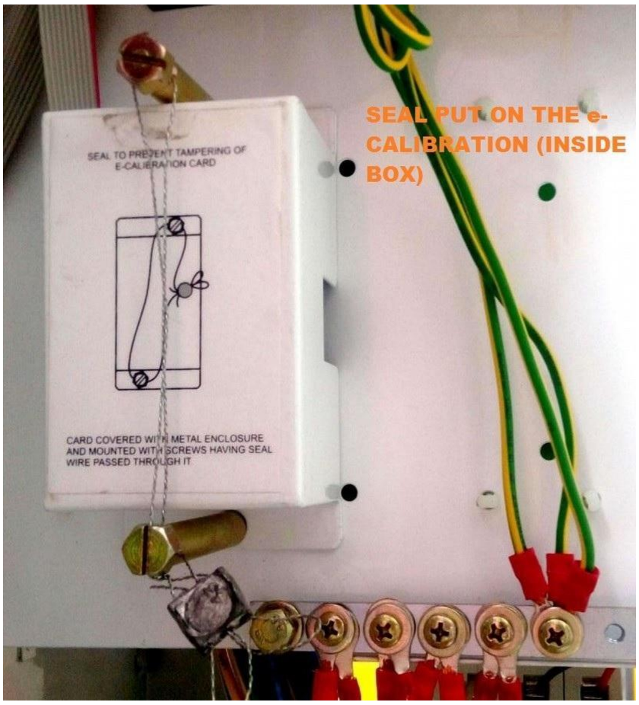

SEAL PUT ON THE e-CALIBRATION (INSIDE BOX)
SEAL TO PREVENT TAMPERING OF E-CALIBRATION CARD
CARD COVERED WITH METAL ENCLOSURE AND MOUNTED WITH SCREWS HAVING SEAL WIRE PASSED THROUGH IT

Fig. 13. Calibration Unit

The original equipment manufacturer shall protect their instrument with the identifying the hardware parts and software. it also provides means through which hardware parts may be supported by software of the equipment. If there is detection of fault detection instrument may be deactivated itself and the record may show error log and in some time alert with alarm. As stated earlier the perceptive description of the detecting algorithm may be with the authenticate algorithm CRC16 is required.

B. Effect of Purchasing the Fuel product by way of denomination of currency 50, 100, 150 etc

- When the customer purchases the quantity with the denomination for refueling 50,100,150 or 200 etc, the DUs will be preset to buttons P1, P2, P3 and P4.
- Some dealers set it to lower value like 99 for 100 or 49 for 50 or 198 for 200 (or may be much lower value). Sometimes short measure can be linked to preset buttons also.
- While customer pay 100 price for petrol will get only petrol for the price of 99 or some lower value, but the display screen will show 100 because that is what they have set the value of 99/98 to be. This will increase the business people profit exponentially.

Retrieval Number: K12870981119/19©BEIESP
DOI: 10.35940/ijitee.K1287.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

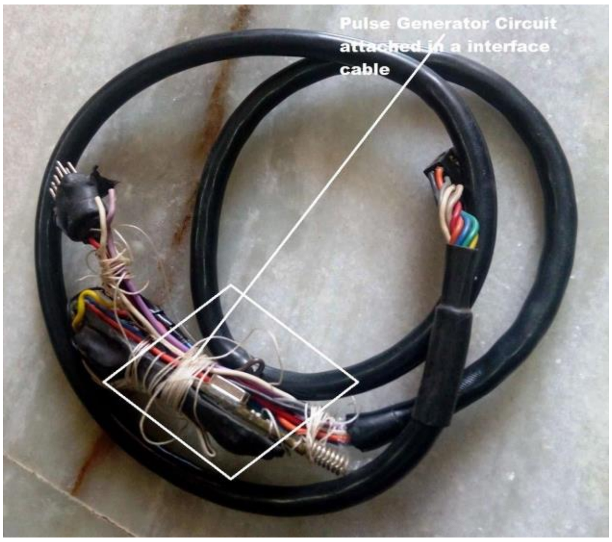


Fig. 14. The remote access chip is inserted in the interface cable.

VII.CALIBRATION FACTOR(K-FACTOR) K-FACTOR GUESSING-PRACTICAL APPROACH

- K-factor is the number of pulses per unit volume.

1) Read only parameter.
2) Unchangeable from external means.
3) Non-editable

- Formulae for New K-factor

$$NewK-Factor = exitingK-Factor * \frac{DispensedVolume\,(in5mlconicalmesure)}{DisplayedVolume\,(onDisplay)}$$

- Generally K-factor is stored in 2 places

1) Permanent storage
2) Control Logic Program

VIII. IMPORTANCE OF ERROR LOG

1) Error log gives the following information such as
   a) Error code
   b) Error description
   c) Date and time
   d) Totalizer value
2) Any change or malpractice happens in the FDU, it must log as an error.
3) Compare the each error with timestamp, the user can easily understand, what are the activities done in FDU.
4) Error log is very important to introspect what happened in the DUs.
5) Take care of E09 and E28.
6) Generally these two errors are produced when external plug-in device is inducted.
7) When doing inspection, retrieving data from error log is like reverse engineering.

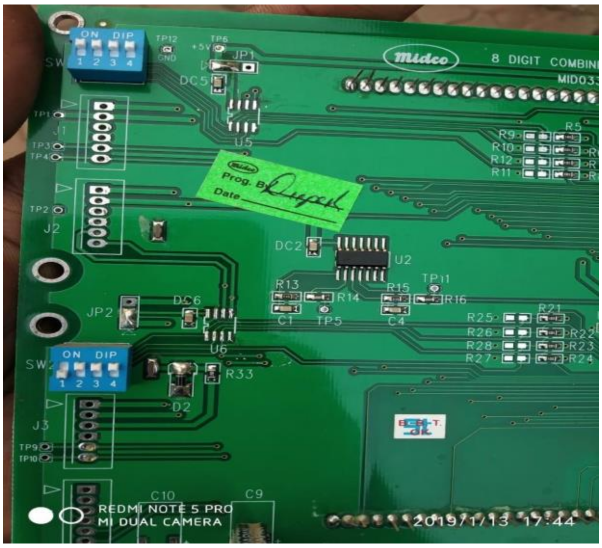


Fig. 15. Midco Mother Board

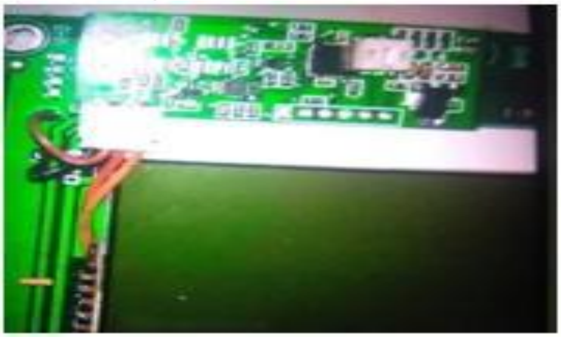


Fig. 16. Bypassing the wires to change the circuit path.

IX.LOGS

1) Log is a collection of information i.e. automatically captured by the system
2) For every operation performed by the dispensing unit a log is generated and saved in permanent storage location.
3) Log contains
   - Log description
   - Data
   - Event
   - Time of transaction

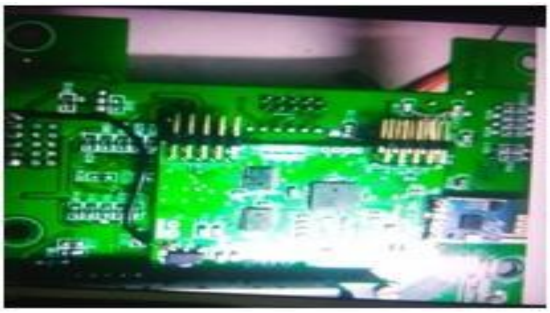


Fig. 17. Wires bypassed with chips to change the circuit path.

Retrieval Number: K12870981119/19©BEIESP
DOI: 10.35940/ijitee.K1287.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

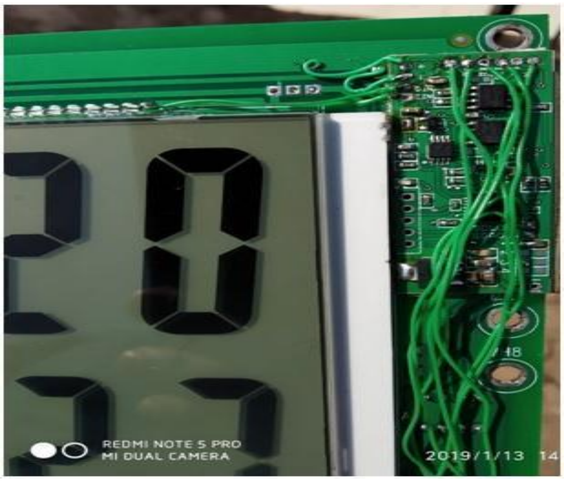


Fig. 18. Bypassing the wires to change the circuit path.

Logs are of two types- System logs and Application logs.

I. SYSTEM LOGS:

1) Asset Identification log
2) Error log
3) Firmware change log
4) Hardware change log
5) OTP usage log
6) Password attempt log

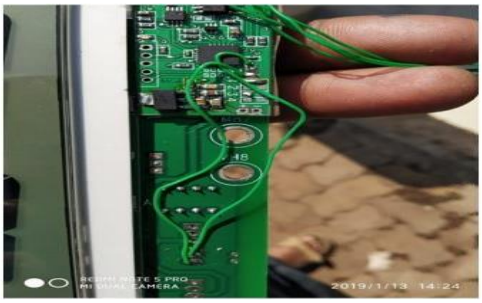


Fig. 19. Changing the chips circuit path by bypassing the cables.

II. APPLICATION LOGS:

1) Calibration Log
2) Date /Time change log
3) Density change log
4) Mode change log
5) Nozzle timeout log
6) Preset sale termination log
7) Price change log
8) Sale transaction Log
9) Test delivery log
10) Totalizer log

X. ENHANCED ROLE OF KEYPAD AND MOTHERBOARD

1) Now-a-days nobody is touching Pulsar, Pulsar cable or communication to motherboard. This is an old phenomenon.
2) Every manipulation on DU is based on Mother board and keypad, external plug-in devices.
3) Thirst of enforcement should be on Motherboard and Keypad.

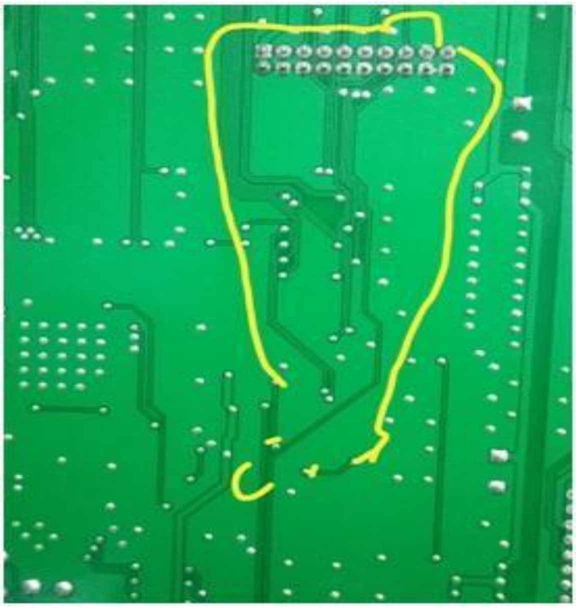


Fig. 20. Modified circuit path which delivers short

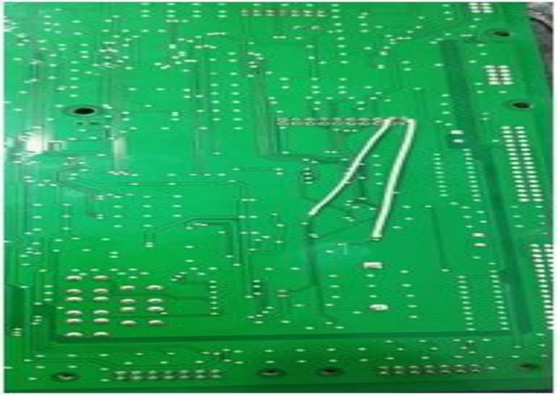


Fig. 21. Modified the circuit path by adding cables with chips

XI. WHICH IS THE EFFECTIVE POPULAR PULSAR PRESENTLY USED

1) Normal Classification of Pulsars
   a) Concealed Pulsar: It is just caged in a steel frame. We cannot open, if we try to open it, it will break. No magnetic pulsar technology or EMF technology is involved.
   b) Potted Pulsar: it is also called magnetic pulsar. EMF technology is involved.

Concealed Pulsar can be differentiated from Potted Pulsar with four openings slots (impractical/ not possible)

Retrieval Number: K12870981119/19©BEIESP
DOI: 10.35940/ijitee.K1287.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

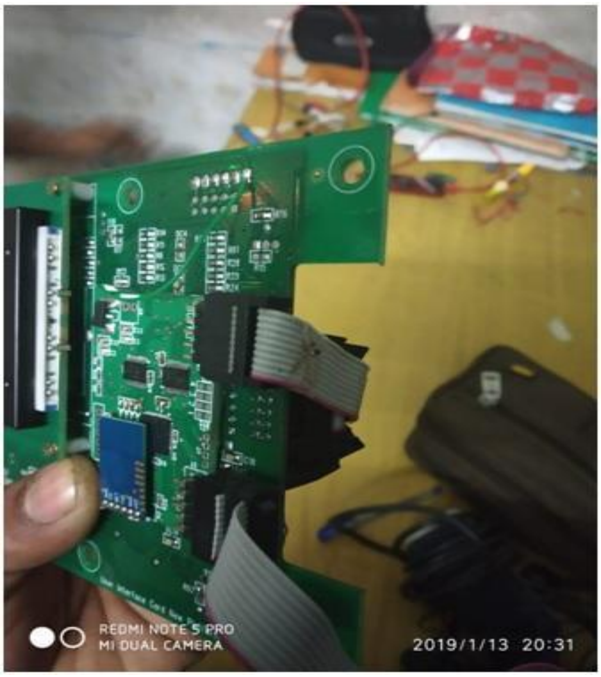


Fig. 22. Bypassing the calibration cable, b. Changing the circuit path by adding cables

2) Technical Classification of Pulsars

a) Optical Pulsars

i) Based on Hall Effect principle.

ii) Varies the output voltage in response to magnetic field.

b) Magnetic Pulsars

iii) Based on Magneto resistive effect.

iv) Its resistor effect depends on electrical resistance on the angle between the magnetization of the ferromagnetic material and directions of the current flow.

v) Only Tatsuno DUs are using this Magneto-resistive based pulsars

XII. ROLE OF NO PRINT NO DELIVERY (NPND)

1) It is complete check for manipulations in MIDCO DUs.
2) Finish one dispensing process, then without printing the receipt FDU will not allow next dispensing.
3) After each dispensing, printing receipt is a mandatory requirement as per the specification, which is called as No Print NO Delivery in both Manual and Auto Mode.
4) Next dispensing will be initiated only after the conformation of the message.

A. Points to ponder before Initial Verification

1) Compare asset identification log with manufacturers manual
2) Compare software version and checksum of DU with manufacturer manual
3) Note down K-factor, Cal count, totalizer readings. Invariably Cal count should be zero.
4) Oil companies are paying for totalizer verification fees also, verify totalizer for at least 20l.
5) Don’t depend for OTP on Technicians.

B. Points to ponder before Initial Verification

1) We shall be equipped with OTP, web app, etc.
2) We have to initiate calibration when we receive OTP in our official mobile only.
3) Legal Metrology should connect with OEM server not only for calibration but for every firmware change.

C. Precautions to be taken while doing Calibration

1) Best weapon for most of the manipulations is Legal Metrology sealing for calibration box communication connector and boot loader.
2) Do inspection- at least 30 days prior to the next renewal date.
3) General tendency is 15 days before calibration renewal date. A culprit normalizes the manipulations.
4) Always mention in Verification Certificate

a) No. of seals and place of seals.

b) If possible take note of unused connectors in motherboard.

c) Always do calibration of your 5l can at least for once in 15 days.

D. Precautions to be taken while doing Calibration

1) In model approval software version and automation software version has to be mentioned.
2) If software update is needed, model approval is a must.
3) While doing calibration please pay special attention to keypad and motherboard on both sides.

XIII. WHAT WE EXPECT FROM OEMS

1) Mention checksum algorithm which was used for calculating checksum of the software version.
2) If possible provide app based checksum calculators.
EX:

a) The most popular checksum integrity verifier is FCIV. Which support SHA-I and MD5 cryptographic hash function.

b) For windows I gorware hasher, it supports MD5,
SHA-1, CRC-32

c) J Digest is open source checksum calculator which works on Mac OS, Windows and Linux.

i) Asset identification ID, including chip wise details with identification number. If we Google the ID number on the chip, you will get chip wise details. You can correlate and come to conclusion.

ii) Supporting manual to retrieve log wise details

3) No. of unused connectors
4) Automation software
5) Every log must grow in incremental form starting from zero.

6) Transparent, plastic for covering motherboard likewise used in Tatsuno.
7) Only one side of the motherboard should be used.
8) Not to entertain mechanical totalizers.
9) Why logs are not generated when one cable is taken out or bypassed are not reflected in logs.
10) Stock Verification in consumer outlets is the need of the Hour to contain totalizer manipulations.
11) While tendering DUs from OEMs, say of Legal Metrology should not be forgotten.

XIV.ERROR CALCULATION OF LPG

- Accuracy Class = 1
- Error = ± 1 %
- While calculating error, we have to determine the Con- version factor from density at present temperature from Master flow meter.

Step1: Note down present density and temperature from MFM. Ex: 0.5465 kg/l at 26.98˚C

Step2: Change these values to ASTM table 53. Ex: 0.560 at

15˚C

Step3: Convert the obtained value to ASTM table 54.
Ex: 0.973 (this is conversion factor)

Step4: Run the dispenser for 5l.

Step5: Note down initial and final reading of MFM

32.7022 - 27.8107 = 4.8915

Step6: Multiply the conversion factor with difference MFM reading

4.8915 ∗ 0.973 = 4.7594

Step7: Error calculation

(4.7594 - 5 ∗ 100) / 4.7594 = −5.055%

XV. ERROR CALCULATION OF CNG

- Error = ± 2 %
- Error calculation method

Step1: Note down initial reading of the MFM (271.2884)
Step2: Run the dispenser for suppose (3.54) kg.

Step3: Note down final reading for MHM (274.9057)

Step4: Calculate difference of initial and final reading of MFM 274.9057 271 - 2884 = 3.6173 kg but dispenser delivered = 3.54 kg

Step5: Error = ((3.6173 - 3.54100) / 3.6173)*100

= 2.13%

We can do zero calibration by connecting laptop with motherboard. Then do not compromise for any deviations.

SUMMARY

These actions obtain the measurement data from the digital sensors in the form of pulses, after calculation of the measurement result; it is displayed on a software window. The data is then passed to the relevant functions and the control is given back to the non-relevant application. The hardware parts shall be protected from the fraudulent use care shall be taken to in the form of hardware and software to minimize the error, while using a universal computer (for example PDA, PC etc.) as the printout as an indication alone may perhaps not be appropriate. Here it is pertinent to mention that the pulse generation card can be manipulated to send the erroneous data by inserting the external devices on the card. The above figure shows that the additional device is fitted in the form of chip in order to give additional pulses which have influence on the end result. Addition of the chips the delivery through the dispenser are altered to the tune of 5.6% by volume as against permitted range of $\underline{+}$0.25%. The microcontroller chips shall be soldered to the motherboard such that rewriting the program in the controller or replacing the spurious microcontroller to the motherboard can be restricted. The biometric applications shall be secured with the three way security with password, fingerprint, and smart card. It can be inferred that the image capturing of Eye i.e., iris method, may be the best biometric system to unlock the electronic device for calibration. The uniqueness of EEG (Electroencephalography) signal can be exploited to remove some of the drawbacks of the existing systems. Secure mobile devices using Electroencephalography signals along with existing pattern based authentication. Electro encephalography signals are modeled using HMM (Hidden Markov Model), and using a binary classifier implemented with SVM (Support Vector Machine) to verify the authenticity of a test pattern. The phonetic password will not help in securing the data. The other problem with the application of the smart phone usage in remote sensing is the adaptability of high level software languages.

XVI.CONCLUSION:

In this work explored the possibilities that are happening at the dispensing pumps and addition circuit that are used to control pumping of the fuel into the customer vehicles through software program that used to controls the outlet unit, alteration possibilities. From this research articles discussion arrived an important point that encryption methods presently available in the microcontroller based are prone to the alteration with external source of hardware hence to make the system robust it should be a better encryption methods incorporated by using the biometric application based to control bit with help of robust software program instead of hardware component by using high-level programming languages that simulate the hardware component and control unit of the outlet pumps.

ACKNOWLEDGMENT

we are very much thankful to the Legal Metrology Statutory officers, Mr.P.Satyanarayana, District Legal Metrology Officer, Medchal Malkajgiri, Telangana State,

Mr.T.Shalem Raju, Assistant Controller, Legal Metrology, Kakinada, Andhra Pradesh State, Mr.B.Praveen Kumar, District Legal Metrology Officer, Sangaredddy, Telangana State, Mr.Sanjay Krishna, District Legal Metrology Officer, Hyderabad, Telangana State for extending cooperation in finding fraudulent practices in the retail outlets of the petroleum products.

REFERENCES

1. Ademir F. da Silva, Ricardo L. Ohta, Marcelo N. dos Santos, Alecio P. D. Binotto, A Cloud-based Architecture for the Internet of Things targeting Industrial Devices Remote Monitoring and Control, Science Direct, 2405-8963 2016, (International Federation of Automatic Con- trol), 10.1016/j.ifacol.2016.11.137.
2. Charles Toth, Grzegorz Jzkw, Review Article Remote sensing platforms and sensors: A survey, ISPRS Journal of Photogrammetry and Remote Sensing 115 (2016) 2236.
3. D. Turecek n, T.Holy, S.Pospisil, Z.Vykydal, Remote control of ATLAS- MPX Network and Data Visualization, Nuclear Instruments and Methods in Physics Research A 633 (2011) S45S47.
4. D. Mourtzisa, V. Zogopoulosa, E. Vlachoua, Augmented reality application to support remote maintenance as a service, in the Robotics industry, Procedia CIRP 63 (2017) 46 51, The 50th CIRP Conference on Manufacturing Systems.
5. Hendri Maja Saputraa, and Midriem Mirdanies, Controlling unmanned ground vehicle via 4 channel remote control, Energy Procedia 68 (2015) 381 388, 2nd International Conference on Sustainable Energy Engineering and Application, ICSEEA 2014.
6. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
7. Ji pale, Remote Motor Control with netX500,
8. J. Saenz F. Esquembre. F.J. Garca, L. de la Torre S. Dormido, A new Model for a Remote Connection with Hardware Devices using Javascript, IFAC-Papers On Line 49-6 (2016) 133137.
9. J. Medina, M. Espinilla, .L. Garca-Fernndez, L. Martnez, Intelligent multi-dose medication controller for fever: From wearable devices to remote dispensers, Computers and Electrical Engineering 0 0 0 (2017) 113.
10. J. Bermudez-Ortega, E. Besada-Portas, J.A. Lopez-Orozco, J.A. Bonache-Seco, J.M. de la Cruz, Remote Web-based Control Laboratory for Mobile Devices based on EJsS, Raspberry Pi and Node.js, IFAC- Papers On Line 48-29 (2015) 158163, 2015, IFAC (International Federation of Automatic Control) 10.1016/j.ifacol.2015.11.230.
11. HardwareX 2 (2017) 112 Adaptable imaging package for remote vehicles Jean-Luc Liardon, D.A. Barry,
12. Kyoung-Yun Kim, Yun Seon Kim, Mark R. Schmeler, Remote decision support for wheeled mobility and seating devices, Expert Systems with Applications 39 (2012) 73457354.
13. L.V. Butov, Excitonic devices, The precise properties of IXs raise a appropriate method for studying fundamental properties of cold bosons and for the advance of signal processing devices based on excitons, Superlattices and Microstructures 108 (2017) 2e26.
14. M. Kozovsky, IFAC-Papers on Line 49-25 (2016) 254259, 2405-8963 2016, 10.1016/j.ifacol.2016.12.043, Remote Programming and Monitoring of Industrial Devices Using NAT Traversal and USB Over IP.
15. Patrick Burgessa, Mohammad Shahidehpour, Mehdi Ganji, Dan Con- nors, The Electricity Journal, Contemporary Strategies for Microgrid Operation & Control, Remote power units for off-grid lighting and urban resilience, The Electricity Journal 30 (2017) 1626.
16. Sergey V. Shavetov, Alexey A. Vedyakov, Anton A. Pyrkin, Alexey A. Bobtsov, Oleg I. Borisov, Advanced educational tool for remote control study, IFAC-Papers On Line 49-6 (2016) 303308.
17. Stefano Tedeschi, Jrn Mehnen, Nikolaos Tapoglou, Rajkumar Roy, Secure IoT Devices for the Maintenance of Machine Tools, Procedia CIRP 59(2017)150155, The Fifth International Through-life Engineering Services Conference.
18. Shraddha Satish Thumsi, Surbhi Jain, Universal Remote Control Sys- tems for Domestic Devices Using Radio Frequency Waves, AASRI Proceedia 9(2014)8-11, Science Direct 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014)
19. Trupil Limbasiya, Nishant Doshi, An analytical study of biometric based remote user authentication schemes using smart cards, Computers and Electrical Engineering 59 (2017) 305321.
20. Unai Hernandez-Jayo, Javier Garcia-Zubia, Remote measurement and instrumentation laboratory for training in real analog electronic experiments, Measurement 82 (2016) 123134.
21. Victor L. Valenzuela and Vicente F. de Lucena, Jr, Remote Monitoring Remote Monitoring and Control of an Electric Powered Wheelchair in an Assisted Living Environment, on-Line 49-30 (2016) 181185, 2405-8963 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved. Peer review under responsibility of International Federation of Automatic Control. 10.1016/j.ifacol.2016.11.164
22. 11th IFAC Symposium on Advances in Control Education June 1-3, 2016. Bratislava, Slovakia Copyright 2016 IFAC 133, IFAC (International Federation of Automatic Control)
23. OIML Specifications D-31 Specifications.
24. Vimal Babu.U, Naga Mani.M , Rama Krishna.M, Review on the Detection of Adulteration in Fuels though Computational Techiniques, Materials Today: Proceedings 4 (2017) 1723-1729.
25. Vimal Babu.U, Naga Mani.M, Rama Krishna.M, Tejaswini. M, Data Preprocessing for Modelling the audulteration detection in Gasoline with BIS, Materials Today: Proceedings 5 (2018) 4637-4645.
26. Vimal Babu U, et all Detection of fuel adulteration through Multivariate Analysis using Python Programming IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 5, Ver. I (Sep - Oct 2018), PP 23-26.
27. Vimal Babu U, Ramakrishna M, Nagamani M, Anjaneya Prasad P, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 06-Special Issue, 2018.

AUTHORS PROFILE

Naagamani.M, Hyderabad did her M.Tech in CS from JNTU, Hyderabad, B.Tech in ECE from JNTU, Ananthapur. She worked in POLICE Communication from 1996 to 2001 and worked as Assistant Professor at Department of IT in GRIET from 2001 to 2007.. She is currently working as Senior Assistant Professor in the School of SCIS., UOH since 2007. Her areas of interest are Embedded System and Sensor Network, Cognitive Sciences, Information retrieval and Signal processing. She has 26 publications in National and International level conference and Journals. She is an associative coordinator for course of P.G. Diploma in Cyber Law and Intellectual Property Right course in CVDL, University of Hyderabad. She is Microsoft Certified Professional

U.Vimal Babu, Hyderabad both B.Tech and M.Tech from Jawaharlal Nehru Technological University, Kukatpally, Hyderabad, India. The author has completed law degree from Osmania University, Hyderabad, Telangana State, India. He has 23 of Experience in the both States government consisting of Andhra Pradesh and Telangana with respect to the enforcement of Legal Metrology Laws. He has 8 publications in National and International level conference and Journals. At present he is working in the rank of Regional Officer in the Legal Metrology Department. He has the duties connected with the enforcement of Legal Metrology Act and Rules made there under. He is having Industrial experience, worked as an Engineer in the Bharat Heavy Plate and Vessels, Visakhapatnam, Andhra Pradesh, India

Dr. Ramakrishna Malkapuram, graduated from V.R.Siddhartha Engineering College. He did his Maters and PhD (Fiber reinforced composites) from IIT Delhi and IIT Roorkee respectively. He is currently working as Dean, IQAC & Professor, Department of Mechanical Engineering, Vignans Foundation for Science, Technology Research (Deemed to be University), Vadlamudi, Guntur Dist., A.P., India, since 2014 and Established Centre of Excellence in Composite Materials. He has 12 PhD students. He worked as a Principal for Various Engineering colleges in present Andhra Pradesh and Telangana States from 2006 to 2014. He has industrial experience as a Supervisor, Production Department, in the Jindal Saw Pipes Division, Nasik from 2000-2002. He had more than 39 Publications in International National journals and conferences.

Sandeep Kumar has Completed MCA and M.Tech (computer Science) both from University of Hyderabad. During M.Tech. project the author has worked on Fuel Aduterants detection using Image processing and IoT. In MCA project he has done project on Investigation of Natural Energy Resources and Demonstration of Solar Energy System. He has conducted 3 day seminar on SCI-lab in CMRIT College Hyderabad. He has also qualified UGC-NET in 2018.