

# Remote Location and Tampering Detection of Domestic Load

Prof. S. A. Thete<sup>1</sup>, A. B. Thete<sup>2</sup>

<sup>1</sup>Department of Electrical Engineering, S.V.I.T. Nashik, Maharashtra, India.

<sup>2</sup>MSTCL, Nashik, Maharashtra, India.

**Abstract**— This paper presents a single phase digital energy meter based on a microcontroller. This digital meter does not having any rotating parts, and the energy consumption can be easily read from a digital display also at remote place we can easily check energy consumption and tampering detection by using GSM technology. When supply will be cut-off, the meter restart with the stored value. Today energy theft is a worldwide problem that contributes heavily to revenue losses. Consumers have been found manipulating their electric meters; try to make them stop, or even bypassing the meter, effectively using power without paying for it. This energy meter has provision to detect tampering in an energy meter by using microcontroller and provide there details at remote location.

**Keywords**— Energy meter, GSM technology, Magnetic Interference, Microcontroller, Tampering.

## I. INTRODUCTION

Today, many electricity distribution companies try to find efficient ways to gather information regarding customers' energy take-off. Traditional method was outdated that when a qualified person knocks at your door and asks for the relevant information. This significant move towards automated data collection opens new doors for telecommunication companies and organizations using classical telephone lines, and wireless technologies. The power distribution monitor is an important research in electric power system, and electricity-stealing defense is one of the chief steps in distribution network reconstruction. Electricity-stealing is a major problem, however, each power supply department has made huge investments of manpower and material, but still electricity stealing methods are improved day by day. Due to the kind of electricity-stealing, and based on a digital single-phase electric energy meter, the metering equipment of electricity-stealing with remote monitoring function is designed, which monitors the time of electricity-stealing and what type of stealing is done, then it will be possible to cut-off supply.[1]

## II. PRINCIPLES OF MEASUREMENTS

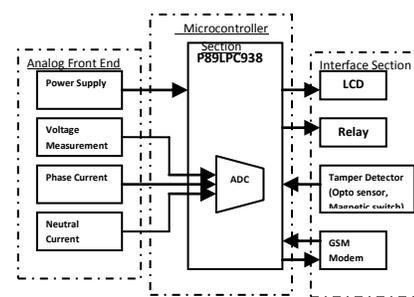
A watt-hour meter is designed to measure energy or power consumed over time. In simple terms, electrical power is the product of voltage and current.

If we make repeated measurements of both instantaneous voltage and current, or  $V_i$  and  $I_i$ , we can keep a calculating total of their products over time. By dividing the total accumulated energy over the number of samples, we have the average power (the first expression in Equation 1). Multiplying the average power by time gives the total energy consumed. [2]

$$\text{Average Power (watts)} = \frac{\sum_{k=1}^N V_{ik} * I_{ik}}{N}$$

$$\text{Energy Consumed (wattsec.)} = \frac{\sum_{k=1}^N V_{ik} * I_{ik}}{F_s}$$

## III. MICROCONTROLLED ENERGY METER DESCRIPTION



**Fig:1 Block Diagram of Digital Energy Meter**

A general overview of the micro controlled energy meter can be seen in the block diagram shown in Fig. 1. As shown the energy meter hardware includes a power supply, an analogue front end, a microcontroller section, and an interface section. We are using a power supply of 3V for the Microcontroller section. +5V and -5v for analog front-end the analogue front end is the part that interfaces to the high voltage lines.

It converts high voltages and high currents to voltages sufficiently small to be measured directly by the analogue/digital converter (ADC) of the microcontroller.

Voltage measurement is done with a potential transformer (PT), while the current measurements require more accurate measurement and it is done by current transformer (CT) on phase along with current measurement on neutral to identify tampering which is basically depends upon phase and neutral current. Microcontroller is heart of the energy meter. Energy calculation is done by P89LPC938 microcontroller.[8] 8-bit microcontroller with accelerated two-clock 80C51 core 8 KB 3 V byte-erasable Flash with 10-bit A/D converter

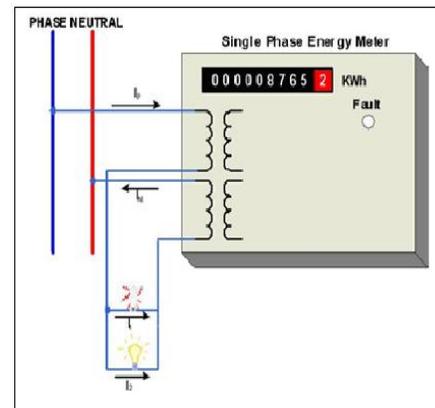
The P89LPC938 is a single-chip microcontroller, available in low cost packages, based on a high performance processor architecture that executes instructions in two to four clocks, six times the rate of standard 80C51 devices. Many system-level functions have been incorporated into the P89LPC938 in order to reduce no. of components, board space, and system cost. In interface section GSM modem is used to transmit data at remote place and also give notification of tampering of energy meter.

#### IV. HACKING IN ENERGY METERS

Due to the increasing cost of electricity, Energy theft is becoming a major concern for government agencies across the globe, and especially in populous countries like India and China. A large portion of these revenue losses can be recovered by installing electronic energy meters because they can detect tampering conditions and assure proper billing, unlike electromechanical meters. This section describes several tampering techniques used by thieves along with solutions for avoiding tampering.[3] The Analysis Of Electricity-Stealing Method is done in following four classifications:-

- A. Stealing electricity by under voltage technology.
- B. Stealing electricity by undercurrent Technology.
- C. Stealing electricity by phase-shifted Technology.
- D. Stealing electricity by difference Expansion (DE) technology.

Figure 2 shows normal Phase and Neutral wire Connection to the meter. Current of the Phase wire is the same as of the neutral wire ( $I_P = I_N$ ). [4]



**Fig:-2 Normal P & N connection**

#### A. Stealing Electricity By Under Voltage Technology:-

**Missing potential:** - This is a common connection fraud usually deployed in meters where the voltage component for one of the phases is made zero by removing one of the phase wires from the meter terminal. This results in recording less energy consumption as consumption from one of the phases becomes zero. During this condition since the voltage is absent and current is present, the logic is easily able to sense this and record as tamper event.[4]

**Bypassing meter:-** There are many ways to bypass an energy meter. The most common way is by putting a jumper in meter terminal such that connection is bypassed and the energy consumption is not registered. This can be avoided by connecting sensor at incoming terminals P & N. [4]

**Powering off meter:** - Meter can be powered off by removing all the voltage connections. [4]

#### B. Stealing Electricity By Undercurrent Technology:-

**Partial earth fault condition:** An earth fault means some of the load has been connected to another ground potential and not the neutral wire. Thus the current in the neutral wire  $I_N$ , is less than that in the Phase or live wire ( $I_P$ ). To detect this condition, firmware monitors the currents on both energy wires - Phase and Neutral, and compares them. If they differ significantly, tampering is detected and notify to remote location. [4]

**Phase and neutral wire swapped:** - In this method live and neutral wires are swapped, which makes the current in the live wire less than that in the neutral.[4]

*Missing neutral:* - The missing neutral tampering condition occurs when the neutral is disconnected from the power meter.[4]

*Double feeding the meter:*- Double Feeding” to bypass the meter where additional feeding is connected directly to the line so that the consumption for additional feeding is not registered. This can be identifying by comparing phase and neutral current. In this Ip is less than In.[4]

*C. Stealing Electricity By Phase-Shifted Technology:-*

*Reverse current:*- Reverse current occurs when the phase and neutral are wired to the wrong inputs, causing current to flow in the direction opposite to normal. When neutral wire connection is swapped then causing current IN to flow in the reverse direction. Due to the reverse current flow through Neutral, metering firmware will show wrong signs in active power readings.[4]

*Neutral disturbance:*- Tampering with the neutral at the source, high-frequency signals are superimposed on neutral causing inaccurate current measurement and thus reducing the energy recorded by the meter. Meter current is also reverse by using inverted supply at source [4].

*D. Stealing Electricity By Difference Expansion (DE) Technology:-*

*High voltage tamper:* - A meter can be tampered with by an electrostatic device that generates spikes or voltages in the range of 35 kV. This may induce errors in consumption recording or may even damage the meter. The accuracy of the meter should not be affected by the application of abnormal voltage/ frequency generating device. [4]

*Magnetic interference:*- Consumers use heavy magnetic material in voltage and current measurement circuits and this are affected by abnormal external magnetic influences that in turn affect proper functioning of the meter. For example, the use of a strong magnet to change the magnitude of current—this in turn introduces large errors in measurement. One way to avoid this is by having magnet sensors to detect the presence of abnormal magnetic fields and provide evidence by logging it as a tamper.[5]

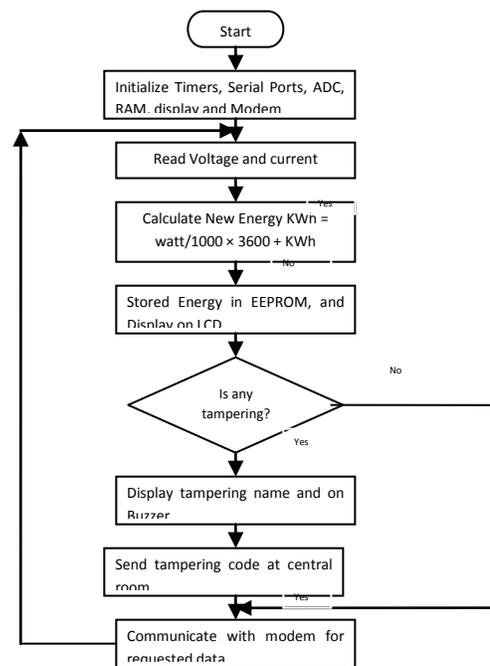
*External crystal connection:*- Electronic energy meter having crystals to generate clock pulses. Tampering is done by connecting external crystal which slows down energy meter. To avoid this tamper select a microcontroller such as having inbuilt clock oscillator.

*External tampers:* - External tampering may include breaking the meter case, chemical injection or even burning the meter. All these result in changing the electrical characteristics of the components thereby recording less or no energy usage.

One may want to open the meter case to change the settings or even remove the backup battery so that the meter will reset when the main power goes off. Anti-tamper switches can be placed on the casing of the meter to trigger a tamper when the casing is opened. [4]

**V. FLOWCHART FOR ELECTRICAL ENERGY MEASUREMENT**

Software is implemented into two major areas, the foreground process and the background process. The background functions use a timer interrupt to trigger the ADC and to collect the voltage and current samples. These samples are further processed and accumulated into buffers [9, 10]. The background function deals mainly with the timing-critical elements of the software. Once sufficient samples have been accumulated, the foreground functions are used to calculate the final values of KWH. The program then enters the main foreground process loop and waits for the timer interrupt routine to gather data.



**Fig: 4 Main flowchart**

**VI. RESULTS**

To validate the proposed energy meter, several experimental tests were carried out. The single-phase prototype was initially calibrated using a 1kW standard load of unity power factor.

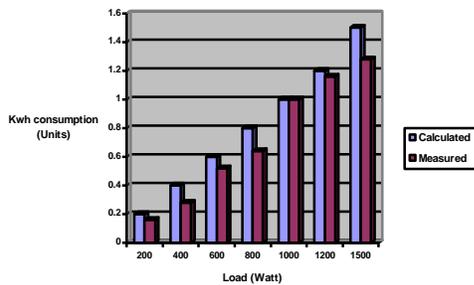
Designed energy meter is shown. Some experimental results were obtained to verify the meter precision.



**Fig:-5 Designed energy meter**

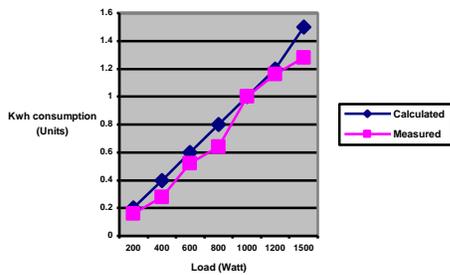
A] Load test at different resistive load and inductive load.

Bar chart of Kwh consumption at various Resistive load.



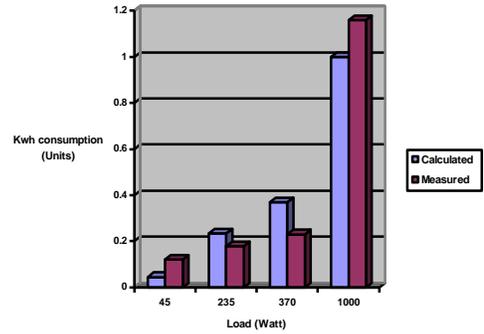
**Bar chart 1:- For resistive Load**

Graph of Kwh consumption at various Resistive load.



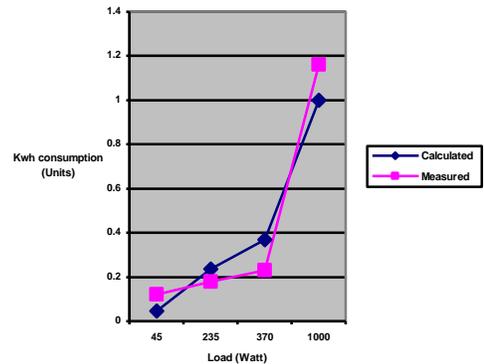
**Line Graph1: - For Resistive load**

Bar chart of Kwh consumption at various Inductive load.



**Bar chart:-2 For inductive load**

Graph of Kwh consumption at various Inductive load.



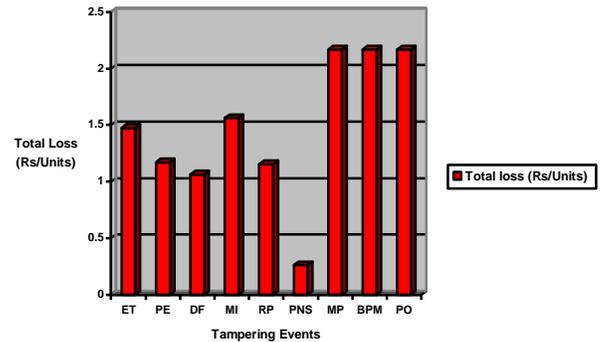
**Line graph2:- For inductive load**

B] Tampering test on different day at 1000watt resistive load.

**TABLE NO I**  
**AVERAGE RESULT TABLE OF ABOVE SIX FOR DAILY LOSS CALCULATION**

Sr. No	Load (watt)	Time (Hrs)	Kwh Consumption		Total Loss (units)	Tampering Method	Total Loss (Rs. 17 /Units)
			Without Tampering (Units)	With Tampering (Units)			
1	1000	1	1	0.32	0.68	External Tamper	1.4756
2	1000	1	0.8	0.26	0.54	Partial Earth (200watt)	1.1718
3	1000	1	0.8	0.31	0.49	Double Feeding (200watt)	1.0633
4	1000	1	1	0.28	0.72	Magnetic Interference	1.5624
5	1000	1	1	0.33	0.67	Reverse Polarity	1.1539
6	1000	1	1	0.88	0.12	P & N swapped	0.2604
7	1000	1	1	0	1	Missing Potential	2.17
8	1000	1	1	0	1	Bypassing Meter{ITT}	2.17
9	1000	1	1	0	1	Powering Off	2.17

Bar chart of Total loss(Rs/Units) in one day for each tampering events.

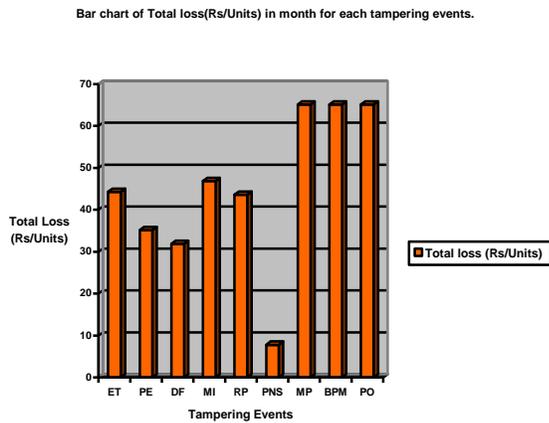


Bar chart:-2 bar chart of Total loss (Rs/Units) at 1000watt load for one day with tampering

From this monthly loss calculation is performed.

**TABLE NO II**  
**MONTHLY LOSS CALCULATION.**

Sr.No.	Tampering Events	Loosed Units/month	Total Loss (Units)	Monthly Total Loss (Rs 2.17 /Unit on basis of Rs. 65.1)
1	External Tamper	$0.68 \times 30$	20.4	44.268
2	Partial Earth	$0.54 \times 30$	16.2	35.154
3	Double Feeding	$0.49 \times 30$	14.7	31.899
4	Magnetic Interference	$0.72 \times 30$	21.6	46.872
5	Reverse Polarity	$0.67 \times 30$	20.1	43.617
6	P & N swapped	$0.12 \times 30$	3.6	7.812
7	Missing Potential	$1 \times 30$	30	65.1
8	Bypassing Meter{ITT}	$1 \times 30$	30	65.1
9	Powering Off	$1 \times 30$	30	65.1



**Bar chart 3:- For monthly loss calculation**

## VII. CONCLUSION

By using GSM technology it is possible to collect energy consumption of consumer without knocking the door of consumer. It turns out that, the system can accurately monitor the behavior of electricity-stealing, giving prompt in time, reduces losses of electricity-stealing to the minimum, decreases country property loss.

## REFERENCES

- [1] MD. Wasi-ur-Rahman, MD. Tanvir Ahmed, Tareq Hasan Khan, and S.M. Lutful Kabir, "Design of an Intelligent SMS based Remote Metering System" Institute of Information and Communication Technology (IICT) Bangladesh University of Engineering and Technology (BUET) Dhaka-1000, Bangladesh
- [2] Paul Daigle,(April 2000) "Digital Energy Meters by the Millions", edition of utility automation.
- [3] Zheng Dezhi, Wang Shuai, "Research on Measuring Equipment of Single-phase Electricity-Stealing with Long-distance Monitoring Function" Electronic measurement technology, 978-1-4244-2487-0/09/2009 IEEE.
- [4] Mohit Arora, (feb. 2009) "Prevent hacking, tampering in energy metres", Freescale Semiconductor, EE Times-India, eetindia.com.
- [5] Margery Conner , "Tamper-resistant smart power meters rely on isolated sensors", march 19, 2009.
- [6] Gaykwad Ramakant A.(2008) "Op-Amps and Linear Integrated Circuits" 4<sup>th</sup> edition. Published by PHI Pvt.ltd, New Delhi.
- [7] P. A. V. Loss, M.M. Lamego, G.C.D. Soma and J.L.F. Vieira "A Single Phase Microcontroller Based Energy Meter" (0-7803-4797-8/98/ 1998 IEEE)
- [8] "UM10119 P89LPC938 User manual" Rev. 02 — 4 March 2005 User manual.
- [9] Muhammad Ali Mazidi, J.G. Mazidi, R. D. McKinly,(2008) " The 8051 Microcontroller And Embedded System".4<sup>th</sup> edition published by Dorling Kindersley(India) pvt. Ltd, licensees of Pearson education in south Asia.
- [10] Stephen Underwood, Frangline Jose, Vincent Chan, Application Report SLAA391–March 2008 "Three-Phase Electronic Watt-Hour Meter Design Using Sp430 .
- [11] Asoke K. Talukder, Roopa R. Yavagal,(2005), "Mobile Computing technology- Application and service creation.",Edition-1.Editor-Prof.H.N. Mahabala, Tata McGRAW Hill Publishing Company Limited, New Delhi.