Design and Fabrication of Smart Digital Energy Meter with Tampering detection and its Mitigation

Aryasupurna Timalsina ^a, Suman Poudel, Arjun Khatiwada, Bibek Prasad Sah, Arbind Kumar Mishra

Department of Electrical Engineering, Pulchowk Campus, Institute of Engineering, Tribhuvan University, Nepal Corresponding Email: ^a timarya123@gmail.com

Abstract

The fact that electricity consumption is undeniably related to the growth of a nation also incorporates the growing need of electricity which also brings power theft like issues. Further the ability to effectively generate electricity by power generation bodies' gets halt when in the process of distribution, energy theft occurs. And with the advent of technology day to day energy meters are also not left as an exception. The use of smart energy meters nowadays has become a compulsion. This paper presents the Design and Fabrication of Smart Digital Energy Meter with Tampering detection and it's Mitigation. The meter comprises with Current transformer (CT), Potential transformer (PT), Arduino as Microcontroller, Liquid Crystal Display (LCD) for user interface and GSM module for wireless communication [1]. The controller calculates the power consumption automatically from sensed voltage and current from PT and CTs respectively, has suitably programmed in C++. The calculated energy consumption is then shown on the LCD display. Multiple circuits' connection is present to implement the logic of tamper detection and mitigation. The system has capability to detect the tamper and warn the consumer. In spite of the tampering, meter functions properly.

Keywords

Microcontroller, Tamper Detection, GSM, LCD

1. Introduction

Energy management system comprises of generation, transmission and distribution of power. Efficiency of whole system depends on efficient functioning of each stage and to increase the efficiency of the energy management system and to cope up with the increasing demand of electricity, the major attention of utilities is to reduce its losses. The losses comprise of technical and non-technical losses. Nepal Electricity Authority's non-technical loss (meter tampering and hooking of lines) currently stands at 9% out of 20.45% average power loss in FY 2017/18. As power system should be designed in such a way that it should have minimum losses, technical losses can't be decrease significantly but with some innovative techniques Non- technical losses could be reduced to certain extent. In response to lower non-technical losses a tamper detecting smart meter can be a good option. Both traditional mechanical energy meter as well as recent digital meter, do not have such features. Addition of Anti Tamper features in Energy Meters can be an effective approach to deal

with major causes of non-technical loses i.e. energy theft related issue. Here this paper shows the relevancy of energy metering formula and further calculates energy consumption digitally. Also different mitigation strategies for tampering problem and GSM based wireless communication module is presented in the paper.

2. Methodology

This paper proposes a smart energy metering system which serves energy metering, tamper detection, tamper mitigation, wireless communication using GSM, and reporting of detected tamper. The system presented here not only depicts anti-tampering feature but also functions properly during tampering period. Further the system possesses features like giving real time data and actual consumption of electricity with wireless communication to the user using GSM [1, 4]. Following are the metering formula which has been used in the system to calculate the energy consumption [4].

$$V_{rms} = \sqrt{\frac{1}{N} \sum_{i=0}^{N} V(i) \times V(i)}$$
(1)

$$I_{rms} = \sqrt{\frac{1}{N} \sum_{i=0}^{N} I(i) \times I(i)}$$
(2)

Active Power =
$$\frac{1}{N} \sum_{i=0}^{N} V(i) \times I(i)$$
 (3)

Energy =
$$\sum_{i=0}^{t}$$
 Active Power $\times t$ (4)

Power Factor =
$$\frac{\text{Active Power}}{\text{Apparent Power}}$$
 (5)

In order to check the relevancy of above metering formula with the theoretical formula certain samples of voltage and current signal were taken.

$$I = I_m \times \sin(wt)$$
$$V = V_m \times \sin(wt)$$

Let,
$$V_m = 311$$
 $R = 1000\Omega$

Theoretically,

$$V_{rms} = 311/\sqrt{2} = 220V$$

 $I_{rms} = 220/1000 = 0.22A$
 $\cos(\Phi) = 1$

Active power (P) = $V_{rms} \times I_{rms} \times \cos(\Phi) = 48.4W$ Apparent power = $I_{rms} \times V_{rms} = 48.4VA$ Power factor = $\cos(\Phi) = 1$

To elaborate the concept of energy measurement, 36 current and voltage signal samples were taken and following analysis was done.

Wt	V(i)	I(i)	$V(i)^2$	$I(i)^2$	$P(i) = V(i) \times I(i)$
0	0	0	0	0	0
15	80.492	0.08	6479.1	0.006	6.479
30	155.5	0.155	24180.35	0.024	24.18
45	219.91	0.219	48360.67	0.048	48.36
60	269.33	0.269	72540.95	0.072	72.54

Table 1:	Samples	of current	and voltage	signals
	Sumples	or current	una vonage	Signais

30 more samples were taken

Using metering formulae, $V_{rms} = 220V$ $I_{rms} = 0.22A$ Active Power = 48.4Watt Apparent Power = 48.4VA Power factor = 1 As a result to relevancy the above metering formula were found valid. So, the metering formulas were used in the system for calculation purpose.

Now, under designing portion of the system, Voltage and Current sensing units, Microcontroller, GSM Module, power supply, rectifier, Relay and Liquid Crystal Display (LCD) were present.

In order to measure the voltage signal a potentiometer was present at secondary of transformer and further the signal was rectified using DC offset mechanism and then fed to microcontroller. Similarly to measure current signal Current Transformer was connected in series with load which was then rectified and fed to microcontroller. Upon receiving both current and voltage signals Microcontroller calculated the energy consumed by the consumer, then checked if any tampering occurred. The system was able to address neutral missing, input output swapping, neutral disturbance, phase neutral swapped and magnetic interference .Similarly to interface between the user and microcontroller regarding information of energy usage and type of tampering occurred GSM module was used.

2.1 Tampering types and its mitigating strategies

2.1.1 Missing Neutral

Missing neutral is a state where value of current is finite but voltage is zero. So, the power is zero. In order to mitigate this problem, then metering firmware is tuned to record voltage equals to 230 V. [1]



Figure 1: Neutral Missing

2.1.2 Neutral Disturbance

Upon introduction of any voltage dropping devices like resistor, capacitor, inductor, diode etc.in the neutral of the source lifts the voltage of the neutral. This decreases the potential difference across the PT giving inaccurate value of power. To mitigate this problem, then metering firmware is tuned to record voltage equals to 230 V.



Figure 2: Neutral Disturbance

2.1.3 Phase and Neutral Wire Swapped

During healthy condition the flux generated by PT and CTs are in same direction and as the phase and neutral wire are swapped the direction of flux generated by PT and CTs reversed but all signals are in same direction. As a result of which average power becomes equal to that of previous.



2.1.4 Input Output Swapping

During healthy condition the direction of flux generated by the PT and both CTs are in same direction But in case of input output swapping flux generated by the CTs is 180° phase out to that of flux generated by PT. This gives average power negative. To mitigate this probelem, absolute magnitude of average power is taken.[2][3]



2.1.5 Partially and Fully Earth Condition

In both the cases the current in the neutral wire IN is less than that the phase wires (IP). To detect this condition, meter monitors the current on both wires IP and IN using two CTs and compares them. If they differ significantly, the meter uses the larger of the two currents to determine the actual energy to be billed and signals a fault condition.



Figure 5: Partially and Fully Earthing

2.1.6 Magnetic Interference

As meters use magnetic material in measurement circuits. Thus, they are affected by abnormal external magnetic interference. Magnetic Reed Switch is used to detect such phenomena. During magnetic interference in energy meter, reed switch closes to give digital high to input of microcontroller. If magnetic tamper occurs then maximum current recorded till date will be assigned as instantaneous current in the billing.

3. Hardware fabricated system



Figure 6: Top view of energy meter



Figure 7: Front view of energy meter



Figure 8: Schematic of the system in proteus

- 4. Findings and Results
- 4.1 Energy meter's response for several loading
- 4.1.1 Incandescent lamp



Figure 9: Incandescent lamp's information and waveform

4.1.2 LED Lamp



Figure 10: LED's information and waveform

4.1.3 CFL Lamp



Figure 11: CFL's information and waveform

Results obtained from energy meter were compared with results from power analyzer.



Figure 12: Power Analyzer

4.1.4 Results from power analyzer

Table 2: Results from Power Analyzer

Load	Voltage	Current	Power	Power
Loau	(V)	(A)	(watts)	factor
Filament (60 W)	219.7	0.263	57.873	0.999
LED (4W)	220.65	0.02367	4.89	0.932
CFL (23 W)	220.6	0.169	21.6	0.597

4.1.5 Results from Energy meter

Load	Voltage (V)	Current (A)	Power (watts)	Power factor
Filament (60 W)	220.63	0.25512	56.312	0.99825
LED (4W)	220.43	0.02351	4.76902	0.91705
CFL (23 W)	221.95	0.16500	21.85114	0.59503

Table 3: Results from Energy Meter

4.2 Energy meter tampering testing

4.2.1 Fully earthed Condition



Figure 13: LCD display for fully earthed condition and waveform

4.2.2 Neutral Missing



Figure 14: LCD display for neutral missing and waveform

4.2.3 Phase and Neutral Wire Swap



Figure 15: LCD display for Phase and Neutral swapped and waveform

4.2.4 Partially Earthed Condition



Figure 16: LCD display for partially earthed condition and waveform

4.2.5 Input Output Swap



Figure 17: LCD display for Input Output swap and waveform

4.2.6 Magnetic Interference



Figure 18: LCD display for Magnetic interference

4.3 Energy meter protection testing



Figure 19: LCD display during overload

During meter overloading, relay operates and breaks the circuit which is indicated by the red LED. A switch on the front panel is pressed to deenergize the relay which reconnect the circuit provided that load is within acceptable limit.

4.4 GSM Communication testing



Figure 20: Billing query and tamper alert message from Data Carrier Unit

5. Conclusion

Upon completion of the project, Design and Fabrication of Smart Digital Energy Meter with Tamper detection and its Mitigation was designed, implemented and tested. The system provided a revolutionary advancement in the technology of energy metering, based on concepts of tampering detection and mitigation, accurate measurements, and wireless communication.

References

- Sarwar Shahidi, Md Abdul Gaffar, and Khosru M Salim. Design and implementation of digital energy meter with data sending capability using gsm network. In 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE), pages 203–206. IEEE, 2013.
- [2] Wessam Mesbah. Detection and correction of tampering attempts of smart electricity meters. In 2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pages 1–6. IEEE, 2016.
- [3] Deepa Warudkar, Priyamvada Chandel, and BA Sawale. Anti-tamper features in electronic energy meters. *International Journal of Electrical, Electronics and Data Communication*, 2(5):114–117, 2014.
- [4] Texas Instruments. TI Training & Videos: Build your own Energy Meter. [Online] https://training. ti.com/build-your-own-energy-meter, March 9, 2015.