ANTI –TAMPER FEATURES IN ELECTRONIC ENERGY METERS

1DEEPA WARUDKAR, 2 PRIYAMVADA CHANDEL, 3 B.A.SAWALE

1,2,3 Central Power Research Institute, Bhopal, India

Abstract- Energy management system comprises of generation, transmission and distribution of power. Efficiency of whole system depends on efficient functioning of each stage. To increase the efficiency of the energy management system and to cope up with the increasing demand of electricity, the main attention of utilities is to reduce its losses. The losses comprises of technical and non technical losses. Several innovative steps to minimize Non-Technical losses (NTL) have been taken by the utilities. Introduction of Anti Tamper features in Energy Meters is one of the ways to bring down the incidence of theft of energy or tampering of meters. Use of Intelligent and smart meters with various Anti tamper features makes electricity theft more difficult and easily detectable. This paper discusses various Anti –fraud measures and tamper prevention methods implemented in electronic Energy Meters.

Keywords- Electronic Energy Meter, Anti-tamper feature, Energy theft, Tampering, Smart meter

I. INTRODUCTION

Utilities experience significant revenue fatalities due to losses. Average power loss in India is more than 26%. Losses of some of the state utilities in the country are more than 30%. Inspite of electrical reforms, these losses have not been significantly reduced. These losses comprise both Technical and Non Technical losses. Technical losses are $I^2R$ power losses and can be calculated. Non technical losses (NTL) are the difference of total losses and technical losses of the system. Non technical Losses occur due to :

a) Tampering with Energy Meter
b) Tapping of Wires on LT lines
c) Ignoring unpaid Bill
d) Delay in meter reading and billing

There are several ways of tampering Energy meter which are adopted by consumers. Newer and newer methods have been cropping up. Utilities are constantly upgrading their specifications to counter the theft and make the meter more immune to theft and also to make the meter intelligent enough to detect the theft. Present days meters have technology to identify the theft and log the tamper with date and time stamping. Meter can keep record of large numbers of tampers, normally 200 tampers in three phase meters and 100 tampers in single phase meters. Meters are also programmed to record the energy at their maximum current rating under certain tamper condition to penalise the consumer or to discourage the consumer from attempting the theft.

Further enhancement of the technology resulting in the Smart Meters, this will help the utility to know the tampering of the meter immediately. Smart Meters are designed to record all the parameters including the detection of the theft and communicate with the Data Concentrator Unit (DCU) at every 10 or 15 minutes time interval. Information from DCU is send to Head End System (HES) and hence the utility can decide to disconnect the consumers load through Smart meters. With this feature, now it is possible for utilities to catch the unscrupulous customers and punish them on the basis of metering data stored in memory of Energy Meter.

Anti- tamper features of Electronic Energy meter is one of the important tools to detect and record the tampering.

II. ANTI –TAMPER FEATURES IN ELECTRONIC ENERGY METERS

Present days meters have following Anti –tamper features are:

a) Phase and neutral interchange
b) Partially or Fully Earth Condition
c) Missing Neutral
d) Neutral Disturbance
e) Missing Potential
f) Bypassing Meter
g) Magnetic Interference
h) External Tamperers
i) High Voltage/Frequency Tamper
j) Jammer
k) Changing the Time

III. TAMPER CONDITIONS AND ANTI TAMPER FEATURES:

Phase and neutral interchange: Phase and neutral of the meter are interchanged then reverse current flows through meter, the meter may read the reverse energy which take off the kWh reading from total reading .The meter with Anti Tamper features activates the reversed current indicator and to overcome this, meter always uses the absolute value for calculation of active power and for driving the energy pulse, thus
reverse current has no effect on energy calculation or accurate billing.

Partially or Fully Earth Condition: In partially earth condition one of the load is connected to earth and other is returned back to neutral of the meter. In fully earth condition the total load is earthed. In both the cases the current in the neutral wire $I_N$ is less than that in the Phase wire $I_P$. To detect this condition, meter monitors the currents in both energy wires - Phase and Neutral with the Measuring C.T. and compares them. If they differ significantly, the meter uses the larger of the two currents to determine energy.

Missing Neutral: The missing neutral tampering condition occurs when the neutral is disconnected from the meter. In this condition, there is no voltage input and thus no output would be generated by the power supply. However when the load is applied, there would be a valid input signal on current circuit, hence power will be consumed. Since the voltage on Neutral is zero, Power $P = V \times I = 0$. This condition is also known as single wire operation.

To take care of this condition, when neutral is disconnected from the meter, meter assumes a fixed voltage at a known amplitude and phase and continues power calculation based on load and produces the same power output as if the voltage is at its normal value. This ensures continuous billing during missing Neutral condition. Most tampering algorithms require current to be measured in neutral apart from all the phases to correctly detect a tamper event and accurately calculate energy consumption.

It is important to measure current in Neutral in addition to Phase currents to detect any mismatch in reverse current flow during the described tamper conditions so that meter can take appropriate steps for accurate energy calculation.

Neutral Disturbance: This is similar to neutral missing except that apart from tampering with the Neutral at the source, High-Frequency (HF) signals are superimposed on neutral causing inaccurate current measurement or by connecting the diode / resistance /capacitor in load neutral circuit of the meter to lift the potential of neutral so that the meter reads less voltage and thus less energy recorded by the meter.

Under this condition like neutral missing, meter assumes fixed voltage at a known amplitude and phase and continue power calculation based on current and record the event as Tamper.

Missing Potential : This is also 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. ($P = V \times I$ where $V=0$)
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 if condition persists for certain duration.

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 kind of meter bypass can be easily detected by monitoring the currents in all energy wires – all Phases and Neutral, and compares them.

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. Here one would have legal service but the meter will not register the consumption for bypass load. Usually the additional feeding is done to connect an appliance that requires more electricity load (like the Air Conditioner). The other loads like lights still go through legal connection so that the electric company will not get suspicious.

Magnetic Interference: Meters use magnetic material in voltage and current measurement circuits and thus are affected by abnormal external magnetic influences, that in turn affect proper functioning of the meter.

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.

Another way to introduced Anti-tamper feature to prevent this type of tampering is that after detection of presence of abnormal magnetic fields by the sensor, meter starts recording energy corresponds to its maximum current rating irrespective of load used. This type of feature introduced in meter to penalise the consumer or to discourage the consumer from tampering the meter.

External Tampering: 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.

To reduce this type of tampering now-a-days meters are ultrasonic welded so that once the meter is opened it cannot be fitted again.

Anti-tamper switches are also placed on the casing of the meter to trigger a tamper and record the Cover Open Tamper with date and time, when the casing is opened.

High Voltage/Frequency Tamper: A meter can be tampered with Tamper device that generates spikes or voltages in the range of approximate 35 kV of undefined Frequency and wave shape. 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. To avoid any influence of 35 kV spike on energy meter a metal plate shielding is provided to house the electronic components and ICs inside the meter.

According to the technical specification of some of the utilities, meters detect this as a tamper condition and starts recording energy corresponding to its maximum current rating to penalise the consumer.

Fig 6.0 35 kV Spark discharge

Fig 7.0 Waveform of 35 kV Spark discharge recorded on CRO

Jammer: With this tamper device high oscillatory waves are generated in a close loop coupled through air with the digital components, which hangs the meter. During this period meter does not record energy. Effect of jammer can be nullified by shielding the complete meter with metallic sheet.
Changing the Time: Electric companies may have different billing rates depending on time of the day, maximum demand, load, etc., thus making a Real Time Clock (RTC) an essential part of the electronic meter to provide time reference. One may tamper with the clock or manipulate the time to fool the system and charge differently, such that metering firmware charges less due to non-peak load during that time. Thus, the RTC circuit should not allow time reversal unless it follows a secure protocol. Meters have a provision to record with date and time the tampering done with the RTC.

IV. Features in Smart Metering to prevent Tampering

Smart Metering provides continuous information about actual electricity consumption by the user, their consumption patterns, identification of abnormal consumption etc. Smart meters are one of the important components of the Advanced Metering Infrastructure (AMI).

These meters are having additional features like a) Connect / Disconnect Facility b) Two way communication. Smart Meters are designed to record all the parameters including the detection of the theft and communication with the Data Concentrator Unit (DCU) at every 10 or 15 minutes time interval. Information from DCU is send to Head End System (HES). HES can analysis the metering data and if any abnormality is noticed in data indicating any type of tampering or theft, utility can decide to disconnect the consumers load through Smart meters or penalise the consumer on the basis of data received from the meter. With this feature, now it is possible for utilities to catch the unscrupulous customers and punish them, which in turn reduces the attempt of tampering with the meter and results in reduction for non technical losses.

CONCLUSION

To reduce the tampering of electromechanical energy meters, Electronic energy meters are introduced. Electronic energy meters are microcontroller based. Many Anti- tamper features are provided that easily detect and record the tamper. Electronic energy meter measures the energy accurately even under tamper conditions and ensures accurate billing even when tampering has occurred unless meter is totally bypassed. Tampering may range from simple techniques like manipulating live or neutral wires to more sophisticated ones like hacking firmware and changing energy consumption records. With the introduction of AMI with smart meters the incidence of tampering will be reduced and the revenue loss of the utilities can be controlled.

REFERENCE:

[1] Mohit Arora, Freescale Semiconductor “Prevent tampering in energy meters” EE Times-India. eeing.com

Author’s Biography: