Freescale Semiconductor
Application Note

Document Number: AN4993
Rev 0, 08/2014

Designing a Tamper Proof Energy Meter Using Kinetis KM34

by: Himanshu Singhal

Contents

1 Introduction

Energy theft is a worldwide problem that contributes heavily to revenue loss. Consumers have been found manipulating their electric meters, causing them to stop, under-register, or even bypass the meter, effectively using power without paying for it. This application note discusses the vulnerabilities, challenges, and techniques to prevent tampering of an energy meter by using the Kinetis KM34 microcontroller.

2 Introduction to energy meters

An energy meter is a device that measures the amount of electrical energy supplied to a residential or commercial building. The most common unit of measurement made by a meter is the kilowatt hour (kWh), which is equal to the amount of energy used by a load of one kilowatt in one hour.

Figure 1 shows a system block diagram for a single-phase energy meter. As shown, the energy meter hardware includes a power supply, an analog front end, a microcontroller section, and an interface section. The analog front end is the interface to high voltage lines. It converts high voltages and high currents to voltages sufficiently small enough to be measured directly by the analog-to-digital converter (ADC) of the microcontroller.

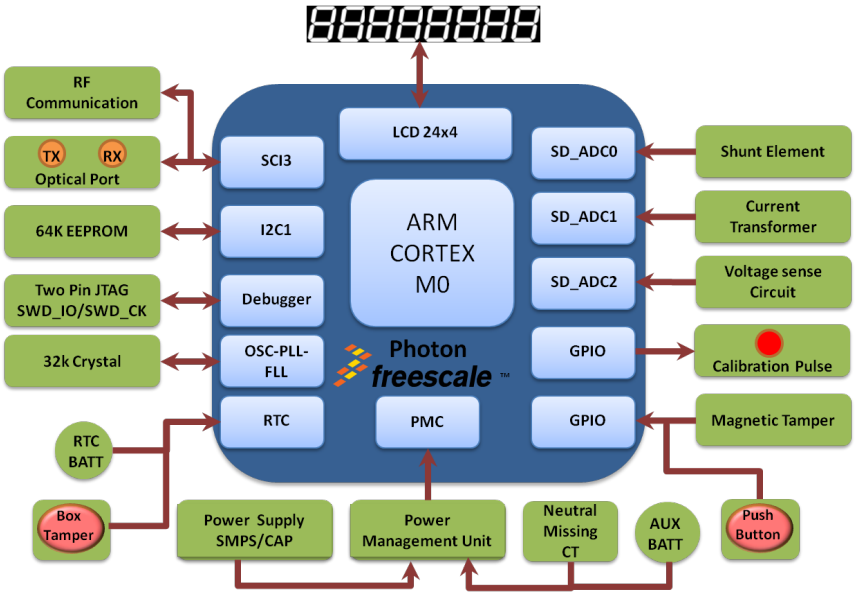

Figure 1. Single-phase energy meter block diagram

Voltage measurements are taken using a shunt resister (shown as “Live”), while the current measurements require more precise measurement and thus are taken using a shunt resistor and a current transformer (CT) on all phases along with current measurement on neutral. Meter manufacturers often integrate gain amplifiers to amplify voltage as well as current measurements in the range supported by the ADC. The amount of amplification required depends on the ADC resolution as well as the class accuracy (0.1, 0.2, 1.0, and so on) required for a three phase meter.

A typical energy meter also requires a real time clock (RTC) for tariff information. The RTC required for a metering application must be accurate to less than 5ppm for time of day (TOD), which divides the day, month, and year into tariff slots. Higher rates are applied at peak load periods and lower tariff rates at off-peak load periods.

The foundation of an electric meter is the firmware, which calculates active and reactive energy based on voltage and current measurement. The firmware also includes tamper detection algorithms, data logging, and protocols such as DLMS and power line modem communication protocol for automatic meter reading (AMR).

The energy meter must be calibrated before it can be used. Calibration occurs in the digital domain for electric meters. Digital calibration is fast, efficient and can be automated, removing the time-consuming manual trimming required in traditional, electromechanical meters. Calibration coefficients are safely stored in an EEPROM that can be either internal or external.

An energy pulse output (EP) is an indication of active power, as registered by the meter; the frequency of the pulse is directly proportional to active power.

3 Hacking energy meters – vulnerability and solutions

Due to the increasing cost of electricity, energy theft is becoming a major concern for government agencies (public utility boards) across the globe.

A large portion of these revenue losses can be identified and therefore recoverd with the installation of electric energy meters because these meters can detect tampering conditions and assure proper billing, unlike electromechanical meters.

This section describes several tampering techniques used by thieves along with solutions to avoid tampering.

3.1 Reverse tamper

3.1.1 Description

Reverse current occurs when the phase and neutral wires are connected to the wrong inputs thus causing current to flow in the opposite direction. Figure 2 illustrates the neutral wire connection when swapped therefore causing current IN to flow in the reverse direction.

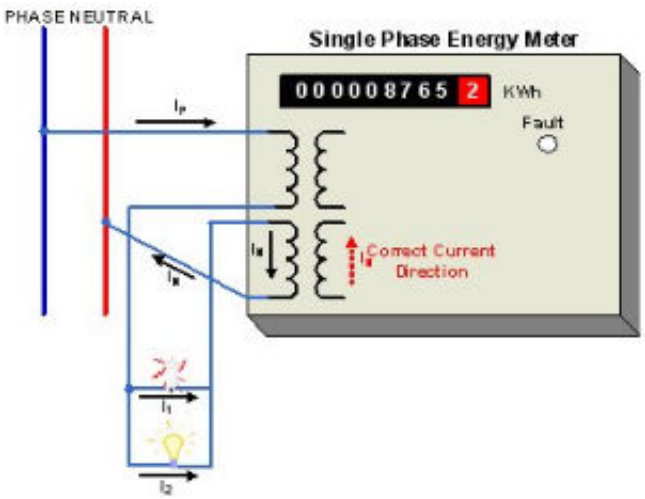

Figure 2. Reverse current due to incorrect wiring connection

3.1.2 Software implementation

When reverse current flow occurs as a result of incorrect neutral wiring, the metering firmware indicates the incorrect signs during active power readings. The firmware activates the reversed current indicator when any of the two currents indicates a sign opposite the one expected. To overcome this, metering firmware always uses the absolute value of active power for driving the energy pulse, therefore, the reverse current has no effect on the energy calculation or accurate billing.

3.2 Earth tamper

3.2.1 Description

An earth fault means that some of the load has been connected to another ground potential and not the neutral wire.

Figure 3 shows the normal phase and neutral wire connections to the meter. Note that the current going through the phase wire is the same as coming out of the neutral wire (IP = IN).

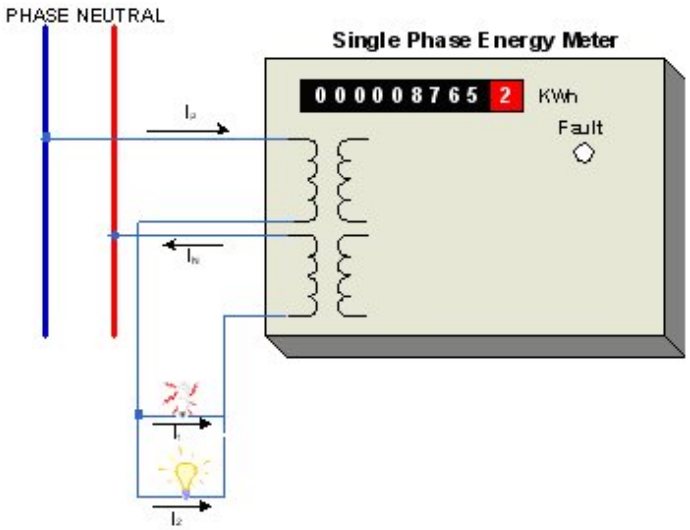

Figure 3. Normal phase and neutral wire connections

Figure 4 shows a partial earth fault condition where one of the loads is connected to ground and thus part of the return current I2 does not go through the meter. Thus the current in the neutral wire IN, is less than that in the phase or live wire (IP).

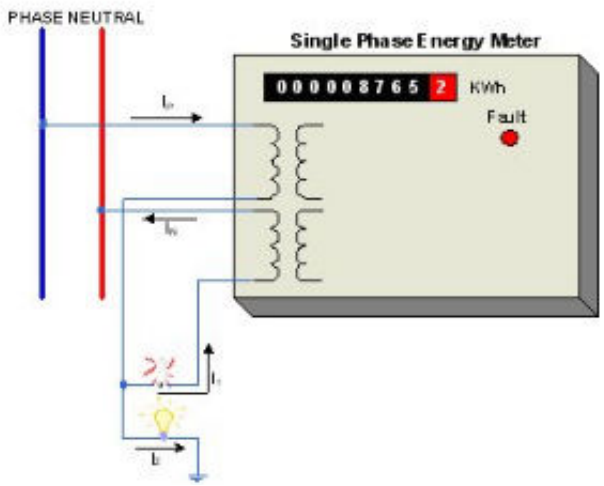

Figure 4. Partial earth fault condition

3.2.2 Software implementation

To detect a partial earth fault condition, the firmware monitors and compares the currents on both energy wires—phase and neutral. If they differ significantly, the firmware uses the larger of the two currents to determine the amount of energy to be billed and signals a "fault" condition.

3.3 Cover open tamper

3.3.1 Description

When the meter casing is opened for the purpose of tampering, modifications to the meter can occur by the following:

- Changing the value of the burden resistance to a lower value so that it measures less current
- Removing the RTC battery

3.3.2 Hardware implementation

A sample implementation of a passive tamper is shown in Figure 5. There is one single-pole double-throw switch. In the default position of the switch, that is, when the meter casing is closed, the switch will be in the state of 0_2 to 1_2. The input on the tamper pin will be seen as 0.

When the meter casing is opened, the switch will be in the state of 0_2 to 2_2 and the input on Tamper will be seen as 1.

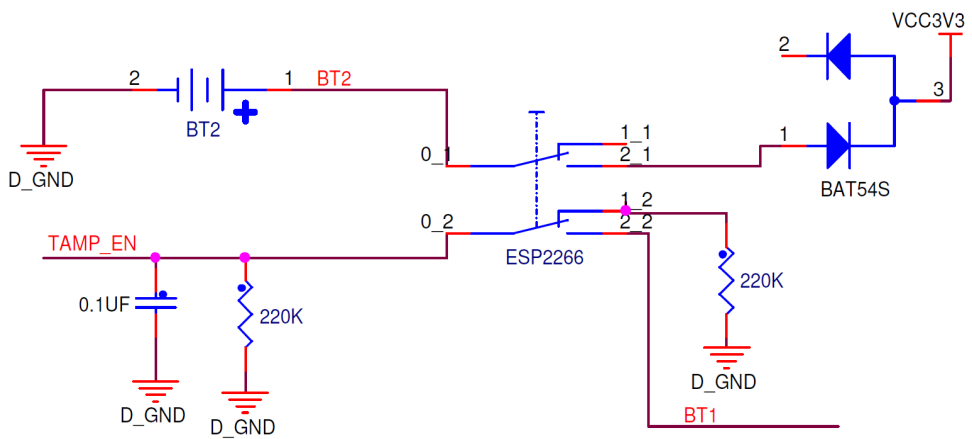

Figure 5. Hardware implementation cover open tamper

3.3.3 Software implementation

As soon as the meter casing is opened, the input on the tamper pin will change from 0 to 1. After the specified filter duration, the tamper event will be recorded and an interrupt will be generated. After the interrupt is generated, required actions such as saving the tamper event in EEPROM can occur.

3.4 Magnetic tamper

3.4.1 Description

Meters use magnetic material in current measurement circuits when current is measured using a current transformer. As a result, these components are affected by abnormal external magnetic influences that in turn affect proper functioning of the meter.

An example of tampering is to use a strong magnet to change the magnitude of current—this in turn introduces large errors in measurement. The idea is to saturate the core of the sensors or distort the flux in the core so that output is erroneous. This effectively results in less billing.

3.4.2 Hardware implementation

The simplest and least expensive method to detect a magnetic tamper is to use magnet sensors to detect the presence of abnormal magnetic fields and provide evidence of such in the form of a digital signal.

The following circuit shows the typical implementation of a magnetic tamper.

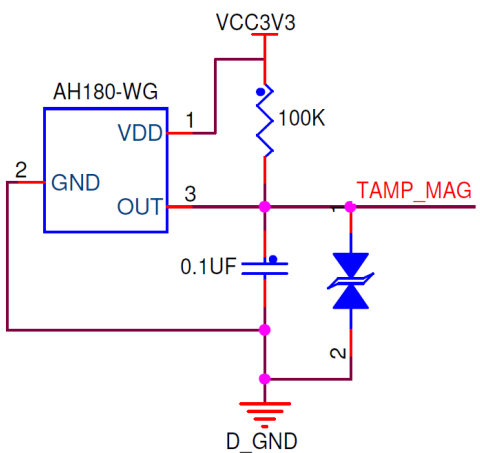

Figure 6. Hardware implementation of a magnetic tamper

The sensor output goes high as soon as the magnetic field intensity is more than 0.2 tesla. The sensor output can be read on one of the tamper pins or on any GPIO pin.

3.4.3 Software implementation

As soon as sensor output goes high, and after validating the state after a period of time, the tamper event is recorded and required actions such as saving the tamper event in EEPROM can occur. Power is calculated on the basis of the rated maximum current multiplied by 240 volts at UPF.

3.5 Single-wire tamper

3.5.1 Description

The single-wire tampering condition occurs when the neutral wire is disconnected from the power meter. When the neutral wire is disconnected, there is no voltage input and thus no output is generated by the power supply. As shown in Figure 7, when the load is applied, normally there is a valid input signal on the current channel so power is consumed. However, because the voltage on the neutral wire is zero, the power is zero (P = V x I).

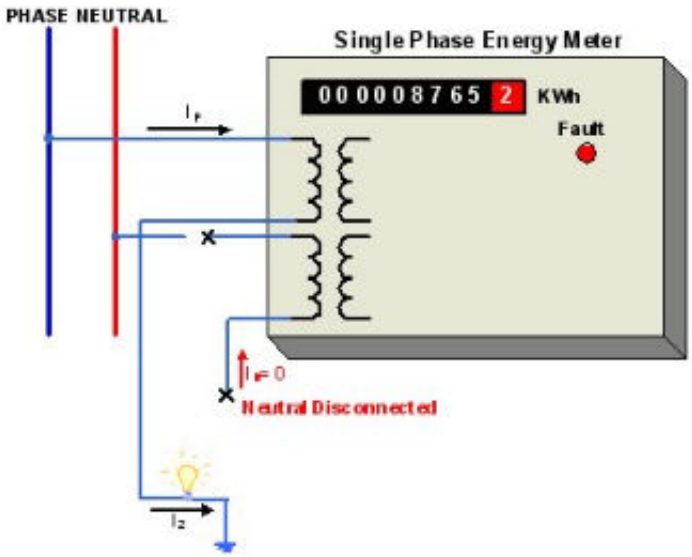

Figure 7. Single-wire tamper

To eliminate this possibility, create a mechanism to power-up the meter through whichever current is present. When the meter is powered-up, the tampering algorithm (part of firmware) assumes the voltage is fixed at a known amplitude and phase and then continues the power-up calculation based on IRMS and adjusts the IRMS gain to produce the same power output when the voltage is at its nominal value. This ensures billing is continued during a missing neutral condition--that is, a single-wire tamper.

3.5.2 Hardware implementation

3.5.2.1 Solution 1: Power-up meter using a current transformer

A typical circuit to power-up the meter in single-wire mode is shown in Figure 8. The meter is powered on using a current transformer. Depending on the turn ratio and the type of power CT used, the required output voltage is obtained.

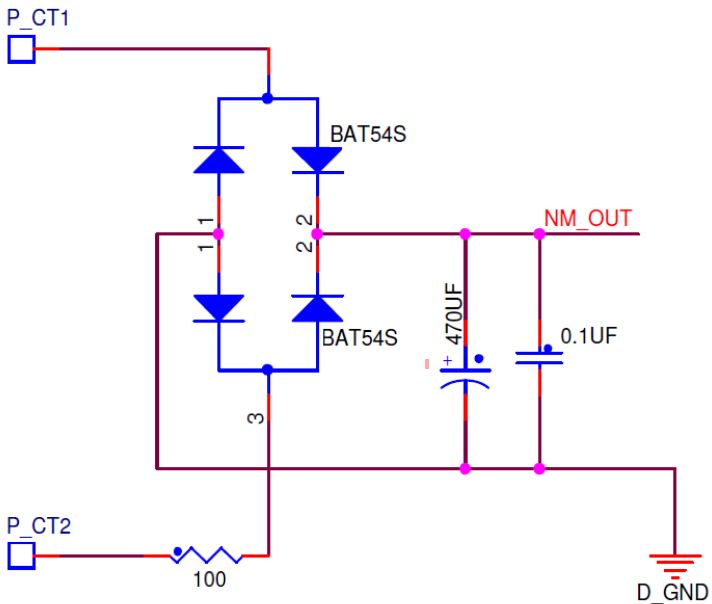

Figure 8. Current transformer to prevent a single-wire tamper

3.5.2.2 Solution 2: Power-up meter using an external battery

In this case, the meter is never powered off. When the main electrical power supply is missing, the meter receives power from the battery and will measure either the phase or neutral current whichever is available.

3.5.3 Software implementation

Solution 1: Power-up meter using a current transformer

In single-wire mode, current is present in either the phase side or neutral side. Depending on which side the current is present, the corresponding current is measured and multiplied by 240 V to calculate the active power. The MCU never enters low-power mode and continuously measures the current.

Solution 2: Power-up meter using an external battery

In this case, the electric meter measures the required current for 1 cycle of the power mains, for example 20 ms, and calculates the energy with the required accuracy. Afterward, the meter goes into deep sleep mode for 1 minute and assumes that the same current will flow for the complete minute. When the minute is over, the meter wakes up and repeats the process. This occurs to maximize the use of the battery so that the electric meter can operate for the desired number of years with lowest capacity of battery.

This can be summarized as:

- Enable RTC to wakeup every 1 minute.
- On wakeup, start the controller in run mode with clock source as IRC.
- Enable one AFE channel to measure current and also enable Vref in low power mode.
- DMA transfers the current samples into a buffer for about 1.25 of mains cycle.
- Go to STOP mode.
- After the desired amount of samples have been collected, the DMA will wake up the system. Disable DMA, AFE and go to VLPR mode and compute energy consumption.
- Now go to VLLS3 mode, the RTC interrupt at the 1 minute boundary will wake the system again.

During this process, the analog comparator is enabled to detect the presence of voltage and re-enable the system into normal mode when voltage is restored.

Kinetis-M features

To start the meter at the lowest input current and to operate with the lowest possible current in a fully functional mode, the power consumption of the MCU must be as low as possible. Using the unique features of the Kinetis-M and the unique optimizations available in software, the required current can be achieved.

The following use case is specific to India and the typical requirements of Indian customers are as follows:

Solution 1:

- The electric meter must be fully functional with the input current of 1A and indicate the required accuracy.
- The required accuracy should be of class 1 throughout the current range.

Kinetis-M features

1. Very low power run (VLPR) mode in which bus clock is restricted to 1 MHz.
2. Operate the AFE in low-power mode.
3. Disable the PGA.
4. Operate the Vref in low-power mode.
5. Enable the only required AFE.

Solution 2:

1. The required accuracy must be class 0.5.
2. The electric meter must be able to run continuously for 5 years on the external battery.

4 Summary

To control revenue losses, utility companies worldwide must detect meter tampering and ensure accurate billing even when tampering has occurred. Tampering ranges from simple techniques such as manipulating live or neutral wires to more sophisticated techniques such as hacking firmware and changing energy consumption records.

The Kinetis KM34 series provides excellent solutions to implement multiple layers of tamper detection through hardware and software solutions.

5 Revision history

Table 1. Revision history

Revision number	Date	Substaitial changes
0	08/2014	Initial release

How to Reach Us:

Home Page:
freescale.com

Web Support:
freescale.com/support

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. Freescale reserves the right to make changes without further notice to any products herein.

Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at the following address: freescale.com/SalesTermsandConditions.

Freescale, the Freescale logo, and Kinetis are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. All other product or service names are the property of their respective owners.

Document Number AN4993
Revision 0, 08/2014