

MCF51EM256 ANTI TAMPER FEATURES A LEAP TOWARDS ROBUST SMART METERING SOLUTIONS

By Mohit Arora, Prashant Bhargava and Stephen Pickering

Energy theft and meter tampering are worldwide problems that contribute heavily to revenue losses. Consumers have been found manipulating their electric meters, causing them to stop or under-register, hacking the meter to alter or stop the internal real time clock, or even bypassing the meter, effectively using power without paying for it. Freescale's latest offering in the metering market segment, the MCF51EM256 microcontroller, provides several anti-tamper features integrated on chip, reducing customer bill of materials (BoM) cost and providing effective protection against tampering.

INTRODUCTION – NEED FOR ANTI TAMPER FEATURES

Due to the increasing cost of electricity, energy theft is becoming a major concern for government agencies (Public Utility Boards) across the globe and especially in populous countries like India and China. In utility metering applications, the hacker might want to extract information and/or modify the internal settings. Many of these methods include tweaking the time so as to fool the system.

Electricity distribution companies may have different billing rates depending on time of the day, maximum demand, load, etc, thus requiring the real time clock (RTC) to provide accurate time reference. One may tamper the clock or manipulate the time to fool the system so as to charge differently, e.g. changing PM to AM such that metering firmware charges less due to non-peak load tariff during the changed time. The RTC usually relies on a 32.768 kHz external crystal oscillator, and a hacker may change the RTC crystal to slow it down so as to count less, thus introducing inaccuracies in measurement and billing.

A large portion of these revenue losses can be recovered by installing electronic energy meters because they can detect tamper conditions and assure proper billing, unlike electromechanical meters. Additionally, as these meters become networked with the introduction of advanced metering technologies like AMR or smart grid, utility companies will benefit by automatically knowing any tampering events that might happen remotely.

ABOUT MCF51EM256

The MCF51EM256 is a ColdFire V1-based MCU with 256 K Flash and includes four high accuracy 16-bit SAR ADCs to measure simultaneously current and voltage on all phases as well as current on neutral. The ADCs are auto-triggered by an

internal programmable delay block to take accurate and in-phase readings for current and voltages. The microcontroller includes an accurate 1.2 V output voltage reference that can be used by internal ADC as well as external components like gain amplifiers for precise measurements. The microcontroller includes an independent RTC (iRTC), which has its own power domain as well as clock and is thus decoupled from the rest of the system. Most of the anti tamper features are implemented in the iRTC. The MCF51EM256 also includes an LCD driver module, a collection of communication peripherals like IIC, SCI, SPI, programmable comparators and AMR SPI/SCI modules.

ANTI-TAMPER FEATURES IN MCF51EM256

RTC with independent power domain

The iRTC is enabled at all the times by running on main supply (VDD) when the main supply is available and automatically switching to battery supply (VBAT) in the event of main power failure. The behaviour is shown in Figure 1.

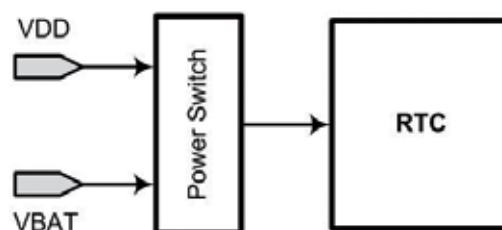


Figure 1 – Independent RTC

The iRTC is capable of detecting the fall in main supply voltage (VDD) to a certain threshold, below which it automatically switches to battery supply. Below this threshold, only the RTC and its oscillator are kept working with the rest of the microcontroller powered OFF.

This allows all the associated logic along with tamper detection (described later) to work in the event of power failure unless the battery is removed or gets drained.

Protection against battery removal or failure

One common way of tampering a system is to remove the battery when the main supply is not available. This allows the hacker to manipulate the system and then connect the battery back as if nothing has happened. The independence of the iRTC includes its reset, clock and power sources. Removal of this independent power source, whilst device powered down, the iRTC is reset when the battery is re-connected and defaults to a tampered state.

It is important to note that the iRTC has a separate “power on reset (POR)” than the SoC POR. The iRTC POR is only asserted for the case where both main and battery supply are removed and either power source is re-connected. The iRTC has the capability to detect removal of the battery and to generate an internal tamper interrupt to the CPU. During the initial meter calibration, this tamper can be ignored as system would be in diagnostic mode.

Detecting tampers external to the system

There could be several attacks that an energy meter may have to face from the real world. These include damage to the casing of the system, alteration of certain signals, etc. The iRTC monitors and detects these intrusions by having support for off-chip anti-tamper switches that can be connected via a dedicated tamper pin on the MCU as shown in Figure 2. Since these anti-tamper switches need to be monitored at all the time, they need to be powered by battery (RTC) supply.

These anti-tamper switches can be prone to noise and can cause false tamper conditions. The iRTC filters out these noises to prevent incorrect triggering.

The tamper event is one of the sources of interrupt to the CPU. The firmware on the event of a tamper can take necessary

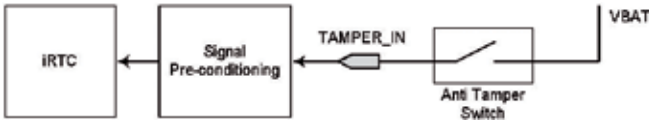


Figure 2 – External tamper detection

actions like erasing any secure information, generating a system reset, storing the tamper event in EEPROM or battery backed registers, and finally clearing the interrupt flag. The CPU response to a tamper event is generally application specific.

It is important to note that once the tamper interrupt is asserted, it cannot be cleared unless both the main (VDD) and battery supplies (VBAT) are removed. When supply is reconnected tamper is the default condition and can only be reset by code within the CPU. For example in the electricity meter, this is normally done during meter calibration.

Additionally, the firmware can implement tamper detection using the internal temperature sensor of the ADC. For example, when the temperature goes beyond a certain operating range or there is rapid change in temperature (i.e. tampering to meter can happen by freezing it or exposing it to a welding torch), the firmware can record such an event in the memory and reported the tamper during meter reading (AMR or manual) and enable the tamper LED.

Time stamping a tamper event

The iRTC can detect the following tamper events:

- Removal of battery when system is on (i.e. VDD is powered ON)
- Removal of battery when system is off (i.e. VDD is powered OFF. Automatically detected by POR)
- External tamper events as described above (e.g. opening of an anti-tamper switch or seal).

The iRTC can record the date (date, month and year) and time (hour, minute, second) in its registers when a tamper event is detected. In an energy meter application, this lets the authorised person who is taking the meter reading know when an attack has happened and the number of times it occurred since installation (via firmware). The energy distribution company can then bill and fine the consumer accordingly. Additionally, the AMR capability helps in quick notification of a tamper event immediately as it happens.

iRTC compensation

The iRTC includes a dedicated oscillator that relies on an external crystal as its clock source for its time keeping operations. This crystal may be subjected to changes in pressure, voltage or temperature, or to certain chemicals that may change the crystal characteristics, thus running the clock slower or faster. The iRTC is capable to compensate for the inaccuracies in the clock and to continue to generate accurate time to the iRTC counters, thus maintaining accurate time. Compensation is done by removal of pulses so as to skip a count if the crystal is running faster or addition of clock pulses if the crystal is running slower. The iRTC can compensate for inaccuracies in the clock from as low as 0.119 ppm to as high as 3906 ppm¹.

Energy meter developers can use the internal temperature sensor of the ADC and maintain the temperature profile of the crystal in system memory to determine the degree of correction needed. The correction in the iRTC is always done over a specific interval called the “compensation interval” and the number of pulses to be added or removed is called the “compensation value.” The firmware must determine these two values and program them in the iRTC registers to perform compensation.

For example, if a change in temperature causes the frequency of 32.768 kHz crystal to reduce then as shown in Figure 3 the

iRTC would actually be counting slow as the period of the resultant 1 Hz clock would increase.

Hence in order to bring the seconds clock (or 1 Hz clock) to the correct value, the iRTC would have to remove clock pulses over specified compensation interval.

Similarly, when the crystal frequency goes on the higher side, the iRTC can be programmed to add the necessary number of oscillator clocks to maintain the correct time.

Firmware may choose to indicate a tamper or crystal failure if compensation that needs to be done is more than acceptable range.

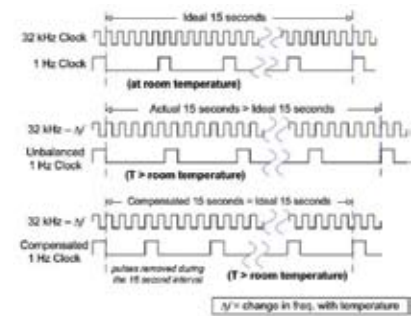


Figure 3 – iRTC clock compensation

Prevent malicious code from changing RTC register settings

All iRTC registers as well as backed-up memory are secured by a write protection mechanism such that any write from a malicious or runaway code cannot change the iRTC register settings unless it goes through a pre-specified unlock sequence.

Figure 4 shows the write protection on the iRTC registers. The registers are unlocked on POR for the first 15 seconds and then get locked automatically. To program them after 15 seconds, a specific sequence needs to be written in the control register which would be known to the valid/secure program only. Once unlocked, the registers would get locked automatically after 2 seconds of unlock. The CPU can optionally lock the registers before the 2 second lapse.



Figure 4 – Write protection sequence

An additional advantage of having this write sequence is to protect the registers against an ESD or external noise that can trigger changes in register settings. Since any write to the register has to go through a fixed sequence, it is highly unlikely that an ESD/noise can corrupt the registers.

Protection against register corruption during low voltage

A hacker may want to reduce the voltage and write to RTC registers so as to corrupt the settings or change values (since the digital logic may not work at that low voltage), thus introducing errors in time. The iRTC is capable of detecting the fall in voltage to a certain threshold below which all write accesses to RTC registers are automatically blocked until the voltage returns to normal operative levels. The CPU is also interrupted in such an event.

Monotonic counting for robust unidirectional count

The iRTC incorporates a unidirectional or monotonic counter that increments on the CPU write cycle when the write condition gets true. This is a 32 bit counter that can be used to maintain the count of energy pulses i.e. in kWh, as a measure of the number of units consumed by the end customer.

This monotonic counter is quite robust against tamper because the counter is cleared only on POR and cannot be re-loaded unless the meter is reset. Every write to it will increment it and hence there is no possibility of it being decremented through any malicious code. Being a part of the RTC register space it is also protected against spurious writes, as explained in previous sections.

Robust firmware code updates

The MCF512EM256 provides efficient and remote update of code, with an option to revert back to old code if needed. The microcontroller houses two blocks of Flash memory each of 128 kB, which are arranged sequentially. Each array has separately mapped Flash registers. Based on a control bit inside the iRTC, the addresses of the two arrays can be swapped. This allows the user to execute from one Flash array while updating the new firmware in the second Flash array. All updates can happen while the microcontroller is in operation. This enables utility companies to update the code remotely without holding any power calculations. For example, if the utility company wants to update the LCD software, the updated software is downloaded into the unused Flash array (Block 1) after un-protecting it. Protection is still enabled on the Flash array (Block 0) from where code is being executed. After updating, the protection on the updated array (Block 1) is re-enabled and the control bit in the iRTC is asserted to point to the Flash array (Block 1) having the updated code. The old code can be erased or left as a fall back option. A reset to the system will cause the new updated code to be executed. In the case a reset is not desired, then the core code must be present in both arrays and must be block protected. The core code will not be modified remotely and entry into background debug mode will be required.

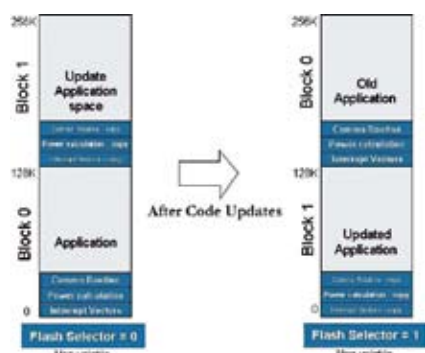


Figure 5 – Firmware upgrade in the MCF51EM256

Figure 5 shows a high level operation of this update process (more detail is available in the MCF51EM256 Reference Manual²).

Automatic meter reading (AMR)

AMR technology refers to the

capability of the meter to communicate its reading to a fully automated collection and communication centre, via the use of wired or wireless networking infrastructure. Some of the AMR technologies employed in various regions around the world include Radio Frequency (RF), ZigBee™ protocol, data modem (via standard telephone network) and power line communication (PLC). Other partial communication may include reading via optical port in an “electronic reader” device. The latter may be based on serial port (RS-485) or infrared link.

With AMR, any tampering events logged in the MCF51EM256 memory can be provided to the substation via the AMR network. The MCF51EM256 implements AMR operation via dedicated SPI/SCI pins available.

Multiple clock sources for fail safe operation

The MCU can be clocked from one of three independent clock sources, the 32.768 kHz iRTC crystal, an external 1-16 MHz crystal, or the internal 32 kHz oscillator as shown in Figure 6. In conjunction with the computer operating properly (COP) with its own independent clock, in the event of a clock failure it is possible to change clock source and maintain normal operation automatically. Oscillators do fail, e.g. solder joint failure, tamper shorting crystal, etc, and in such an event, the system would freeze but the COP would continue to run on its independent

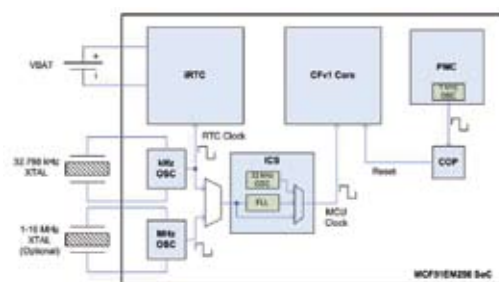


Figure 6 – Multiple clock sources for fail safe operation

clock and generate a reset on timeout. The system can choose to change the clock source, i.e. switch to the internal clock

source during re-boot after the reset.

Although the internal oscillator is of lower accuracy, it is better to measure energy at lower accuracy than not to measure at all. Any clock failures can be reported during meter reading (AMR or manual). A tamper log can be created with a clock failure and enable the tamper LED.

Meter tampering

There are several ways in which a meter can be hacked or tampered with. Readers are encouraged to read the article on “Prevent tampering in energy meters”³ that provides lot of meter tampering methods along with countermeasures.

SUMMARY

In a smart grid, energy metering products enable two-way communication with the utility companies, which allows remote access and control of these devices. With human monitoring/control (from the utility company side) becoming less, it is all the more important that these devices are strong enough to tolerate tampers and are secure enough to handle sensitive information about the consumer. The MCF51EM256 microcontroller is an efficient solution that can very well cater to these needs and most other smart metering needs of today and the future.

The MCF51EM256 is well suited for metering applications specifically single phase and poly phase energy meters, both networked as well as non-networked. All the above mentioned features have been implemented in poly phase energy meter reference design based on the MCF51EM256. **MI**

References

1. A “Stitch” in Time: Accurate Timekeeping with On-Chip Compensation – Prashant Bhargava, Mohit Arora, IEEE VLSI Conference, 2009 (<http://www.computer.org/portal/web/csdl/doi/10.1109/VLSI.Design.2009.70>)
2. MCF51EM256 Reference Manual & Datasheet (www.freescale.com)
3. Prevent Tampering in Energy Meters – Mohit Arora, Freescale Semiconductors, Industrial Control Design Line (<http://www.industrialcontroldesignline.com/howto/213000906>)



ABOUT THE AUTHORS:

Mohit Arora is a Systems Engineer in Freescale Semiconductors. His current focus is on the energy/utility metering market. He has been involved in product definition and specification for ColdFire/PowerPC based products for mid-high end industrial market space. He earned a Bachelor’s degree in Electronics and Communication Engineering from Netaji Subhas Institute of Technology, India.



Prashant Bhargava is a Design Lead in Freescale Semiconductors and has worked in design and architecture of microcontrollers for different applications like VoIP, display controllers and utility metering. He holds a Bachelor of Engineering degree in Electronics & Communication from Punjab Engineering College, Chandigarh, India.



Stephen Pickering is a Systems Engineer in Freescale Semiconductors. His work involves the architectural definition of micro-controllers for various application, and he has spent the last 2-3 years defining solutions for utility meters and has visited over 40 different meter manufactures worldwide during the definition of current and future micro-controllers.

ABOUT THE COMPANY:

Freescale Semiconductor is a global leader in the design and manufacture of embedded semiconductors for the automotive, consumer, industrial and networking markets. The privately held company is based in Austin, TX and has design, research and development, manufacturing and sales operations around the world. Freescale is one of the world’s largest semiconductor companies with 2008 sales of \$5.2 billion. www.freescale.com