Freescale Semiconductor
应用笔记

Document Number: AN4993
Rev 0, 08/2014

利用 Kinetis KM34 设计防篡改电表

作者: Himanshu Singhal

内容

1 简介 1
2 电表简介 1
3 侵入电表—漏洞与解决方案 2
4 总结 8
5 修订历史记录 8

1 简介

窃电是一个会导致严重经济损失的全球性问题。某些用电者通过篡改电表使其停止工作、计量不足甚至避开计量器，以达到免费用电的目的。本应用笔记将会讨论电表应用中的这些设计难题，以及利用 Kinetis KM34 微控制器来防止篡改的技巧。

2 电表简介

电表是用来测量住宅或商业楼宇供给电能的设备。电表测量中最常用的单位是千瓦时(kWh), 相当于 1 千瓦负载运行 1 小时所使用的电能。

图 1 显示了单相电表的系统框图。如图所示，电表硬件包括电源、模拟前端、微控制器部分和接口部分。模拟前端是连接高压线的接口。它将高电压和高电流转换为可由微控制器上的模数转换器(ADC)直接测量的小电压。

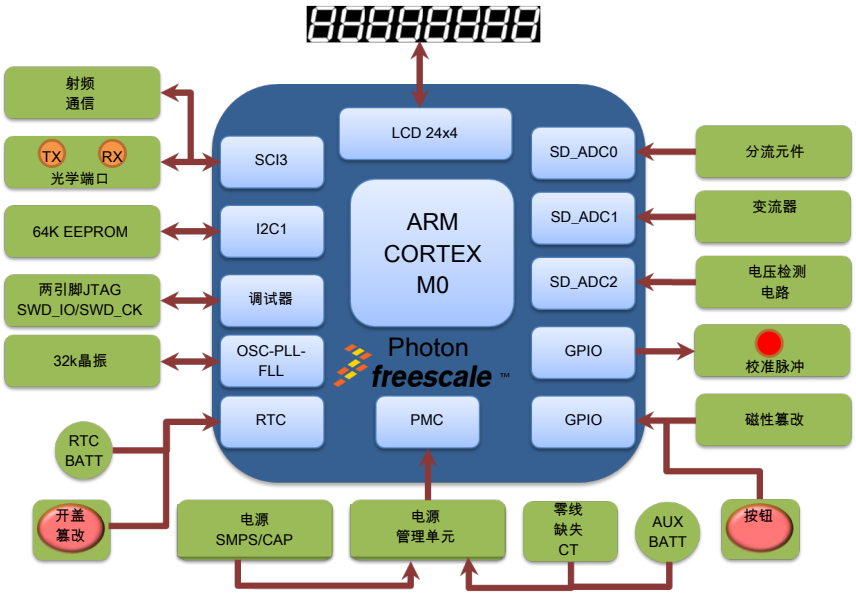

图 1. 单相电表框图

电压测量通过分流电阻（显示为“Live”）实现，由于电流测量需要更为精确的手段，因此对各相电流使用分流电阻与变流器(CT)，并进行零线电流测量。仪表制造商通常会在电表中集成增益放大器，用于在 ADC 支持的范围内放大电压与电流的测量。所需的放大量取决于 ADC 分辨率和三相电表所需的等级精度（0.1、0.2 和 1.0 等）。

典型的电表还需要实时时钟(RTC)用于收费信息。计量应用所需 RTC 的精确度必须达到时间信息(TOD)误差小于 5ppm，用于将年月日分别计入不同的费用分类中。处于峰值负载周期时的费率较高，非峰值负载周期时的费率就较低。

固件是电表的基础，可基于电压和电流测量计算有功与无功电能。固件中还包含篡改检测算法、数据记录和协议，如 DLMS 和用于自动仪表读取(AMR)的电力线调制解调器通信协议。

在使用电表前必须对其进行校准。校准在电表的数字模块部分中进行。数字校准速度快、效率高，并可以自动化，省去传统机电式电表所需的耗时手动调整方式。校准系数存放于内部或外部 EEPROM 中。

能量脉冲输出(EP)可用来指示有功功率，由电表记录；脉冲频率与有功功率成正比。

3 侵入电表—漏洞与解决方案

由于电力成本的不断增加，窃电问题正逐渐成为全球政府机构（公共事业局）关注的重大问题。

安装电能表可识别并挽回这方面大部分的经济损失。这种电表与机电式电表不同，可以检测篡改状态并确保正确的计费功能。

本章节描述了窃电者常用的几种篡改手段及防止篡改的解决方案。

3.1 反向篡改

3.1.1 说明

当相线与零线连接到错误的输入时就会发生反向电流，从而导致电流从反方向流入。图 2 显示交换后的零线连接导致电流 IN 流向相反方向。

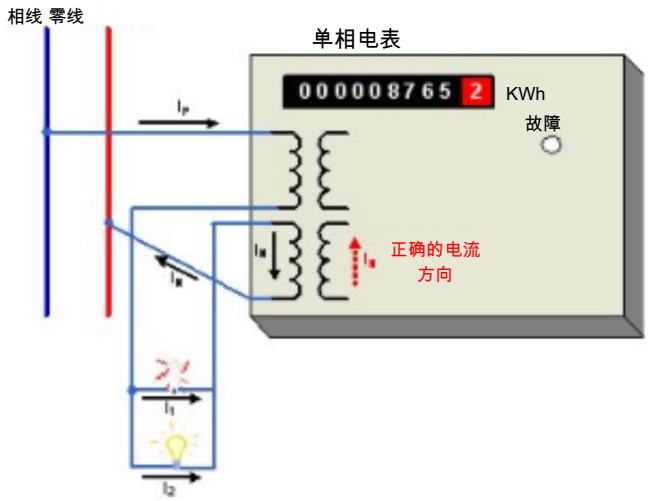

图 2. 由于错误连线导致的反向电流

3.1.2 软件实现

当由错误的零线连接导致反向电流发生时，仪表固件会在有功功率读取时指示出错误信号。当两个电流中的任一电流显示出与期望相反的方向时，固件会激活反向电流指示器。为了克服这个问题，仪表固件总是使用驱动能量脉冲的有功功率绝对值，因此反向电流对能量计算或准确计费没有影响。

3.2 接地篡改

3.2.1 说明

接地故障意味着一些负载被连接到其他地电位而非零线。

图 3 显示了相线和零线与电表之间的正常连接。注意，通过相线的电流与零线的电流相同(IP = IN)。

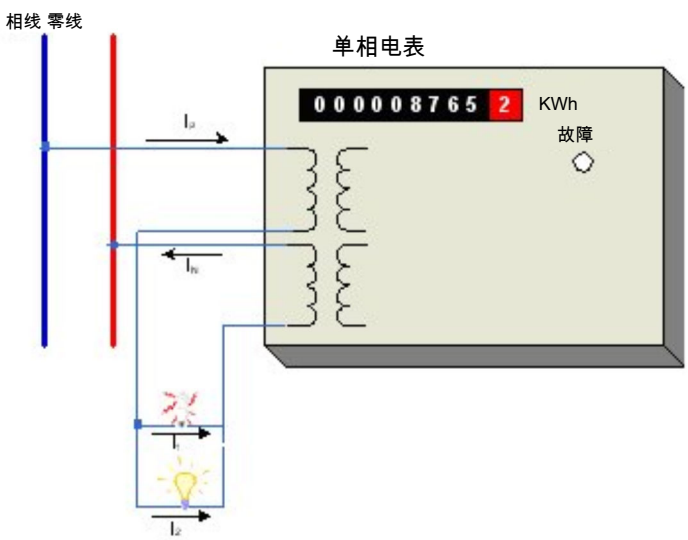

图 3. 相线和零线的正常连接

图 4 显示了一种部分接地故障的情况，其中一个负载连接到地，因而部分返回电流 I2 不经过电表。所以零线中的电流 IN 小于相线或火线电流(IP)。

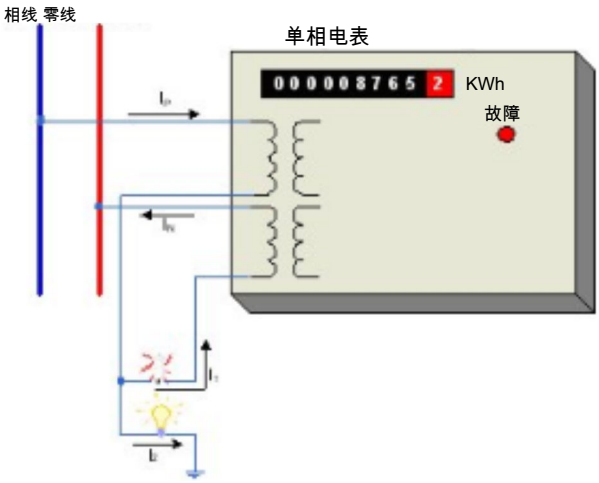

图 4. 部分接地故障的情况

3.2.2 软件实现

要检测部分接地故障的情况，固件会监测并比较两根能量线—相线和零线上的电流。如果它们之间的差别很大，则固件会使用其中较大的电流来确定耗电量并计算费用，同时发出“故障”情况信号。

3.3 开盖篡改

3.3.1 说明

当电表外壳由于篡改目的而被打开时，可能发生以下电表修改:

- 减小负载电阻值，从而减少测量电流
- 移除 RTC 电池

3.3.2 硬件部署

图 5 显示了针对被动篡改的部署示例。这是一个单刀双掷开关。开关处于默认位置，即电表外壳关闭，开关将处于 0_2 至 1_2 状态。篡改引脚上的输入将为 0。

当电表外壳打开，开关将处于 0_2 至 2_2 状态，篡改引脚上的输入将为 1。

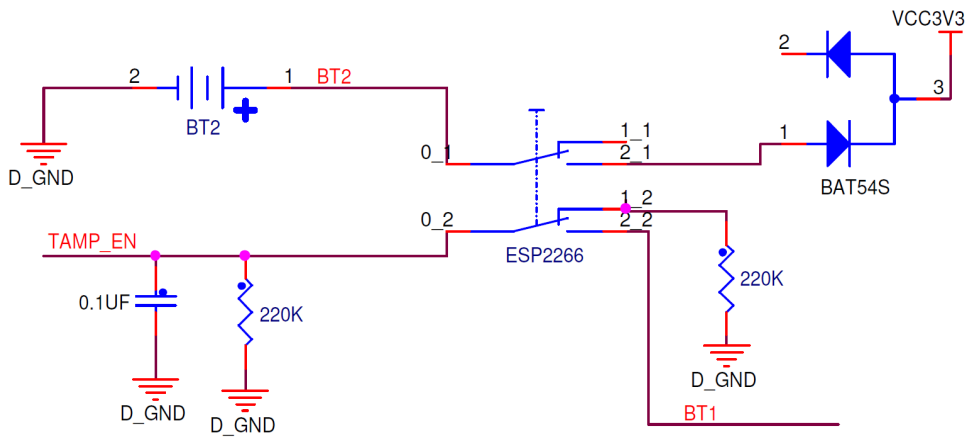

图 5. 针对开盖篡改的硬件部署

3.3.3 软件实现

一旦电表外壳打开，篡改引脚上的输入就会从 0 变为 1。在指定滤波器持续时间后，系统将记录篡改事件并产生中断。中断产生后，就可以进行所需的动作，如将篡改事件存入 EEPROM。

3.4 磁性篡改

3.4.1 说明

若利用变流器测量电流，则电表的电流测量电路中会使用磁性材料。这些元件易受外部异常磁干扰的影响，从而影响电表的正常功能。

一种篡改示例是使用强力磁铁来改变电流幅度—这会向测量中引入巨大的误差。其意图是使传感器磁芯饱和或扭曲磁芯的磁通量，导致输出错误，从而减少所计的电费。

3.4.2 硬件部署

检测磁性篡改最简单、经济的方法是使用磁性传感器来检测是否存在异常的磁场，并以数字信号的形式提供证明。

以下电路显示了针对磁性篡改的典型部署。

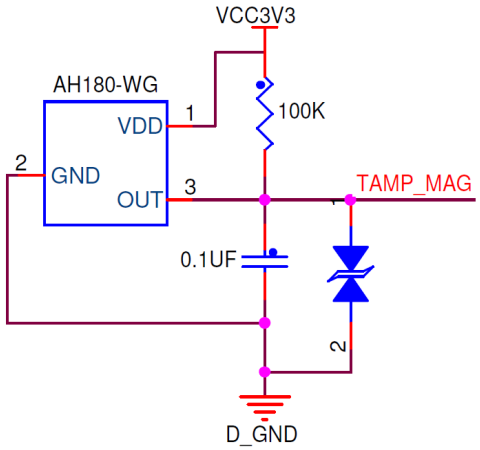

图 6. 针对磁性篡改的硬件部署

一旦检测到磁场密度高于 0.2 T，则传感器输出高电平。可通过一个篡改引脚或任意 GPIO 引脚读取传感器的输出。

3.4.3 软件实现

一旦传感器输出高电平，并且持续一段时间验证状态后，系统将记录篡改事件并执行所需动作，如将篡改事件保存到 EEPROM 中。功率计算基于额定最大电流乘以 240V (UPF)。

3.5 单线篡改

3.5.1 说明

单线篡改情况发生在零线从电表断开时。当零线断开时，将没有电压输入，因而电源不会产生输出。如图 7 所示，当应用负载时，电流通道上通常会存在有效的输入信号，从而消耗能量。然而，由于零线上的电压为零，则功率为零(P = V x I)。

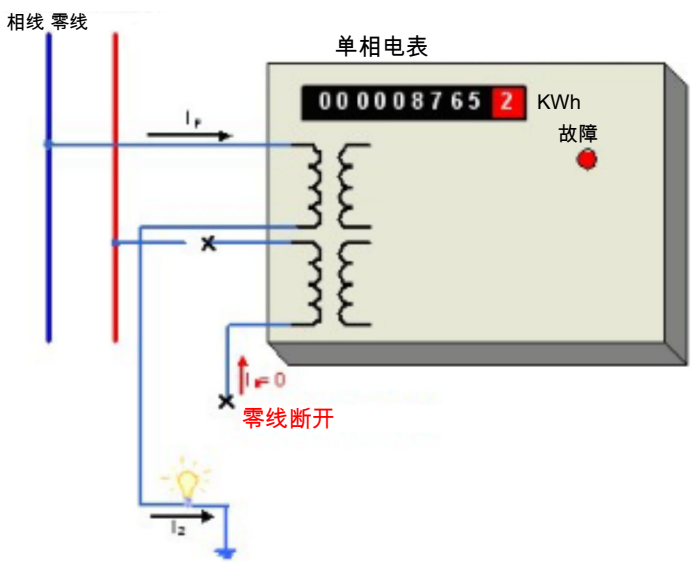

图 7. 单线篡改

为避免这种情况，应创建一种机制使电表可通过任一电流通电。当电表通电时，篡改算法（固件部分）假设电压处于已知的幅度和相位，基于 IRMS 继续进行通电计算，并调整 IRMS 增益使其功率输出与电压处于额定值时相同。这确保了在零线缺失（即，单线篡改）的情况下仍可继续计算费用。

3.5.2 硬件部署

3.5.2.1 解决方案 1：利用变流器对电表供电

在单线模式下对电表供电的典型电路如图 8 所示。该电表通过变流器供电。根据匝数比和变流器的功率类型，可以获取所需的输出电压。

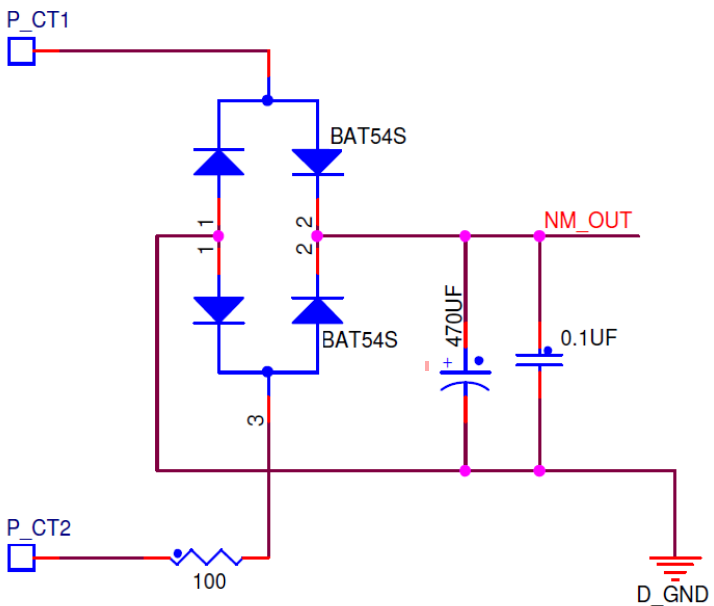

图 8. 使用变流器防止单线篡改

3.5.2.2 解决方案 2：利用外部电池对电表供电

这种情况下，电表将永不掉电。当主电源缺失时，电表会由电池供电，并测量可用的相电流或零电流。

3.5.3 软件实现

解决方案 **1**：利用变流器对电表供电

在单线模式下，电流或存在于相线侧，或存在于零线侧。根据电流所处的位置，测量相应电流并乘以 240 V 以计算有功功率。MCU 永不进入低功耗模式并将持续测量电流。

解决方案 **2**：利用外部电池对电表供电

在此情况下，电表测量主电源在一个周期的所需电流，例如 20 ms，然后根据要求的精确度计算能量。之后，电表进入深度睡眠模式并持续 1 分钟，假设在此期间流过的电流相同。这一分钟结束后，电表唤醒并重复之前的过程。这种方式可对电池进行充分利用，通过极少的电池电量即可使电表的运行时长达到理想年数。

该解决方案可以总结为：

- 启用 RTC 以每分钟唤醒一次。
- 唤醒时，在运行模式启动控制器，时钟源为 IRC。
- 启用一个 AFE 通道以测量电流，并在低功耗模式启用 Vref。

- DMA 将电流采样信号传入缓冲器，大约需要 1.25 个主电源周期。
- 进入 STOP（停止）模式。
- 在集齐所需的采样数量后，DMA 将唤醒系统。禁用 DMA 和 AFE，进入 VLPR 模式并计算功耗。
- 现在进入 VLLS3 模式，在一分钟边界处的 RTC 中断将再次唤醒系统。

在此过程中，启用模拟比较器来检测电压，并在电压恢复后重新使系统进入正常模式。

Kinetis-M 特性

为了在最低输入电流的情况下启动电表，并在全功能模式下以最低可能电流工作，MCU 的功耗必须尽可能的低。利用 Kinetis-M 独有的特性与软件优化，可实现该低电流要求。

以下用例适用于印度，印度客户的典型需求如下:

解决方案 **1**:

- 电表必须功能齐全，输入电流为 1 A，并能指示要求的精确度。
- 在整个电流范围内的要求精确度应为等级 1。

Kinetis-M 特性

1. 支持超低功耗运行(VLPR)模式，其总线时钟限制为 1 MHz。
2. 在低功耗模式下操作 AFE。
3. 禁用 PGA。
4. 在低功耗模式下操作 Vref。
5. 启用所需的 AFE。

解决方案 **2**:

1. 所需精确度必须为等级 0.5。
2. 电表采用外部电池必须能够连续工作 5 年。

4 总结

为了控制经济损失，全球的水电公司必须检测仪表篡改情况，并确保仪表在篡改发生时仍能准确计费。篡改方式包括简单手段（如修改火线或零线）和复杂手段（如侵入固件和修改能耗记录)。

Kinetis KM34 系列提供出色的解决方案，通过硬件与软件解决方案实现多层面的篡改检测技术。

5 修订历史记录

表 1. 修订历史记录

修订版本号	日期	重要改动
0	08/2014	初始版本

How to Reach Us:

Home Page:
freescale.com

Web Support:
freescale.com/support

本文档中的信息仅供系统和软件实施方使用 Freescale 产品。 本文并未明示或者暗示授予利用本文档信息进行设计或者加工集成电路的版权许可。 Freescale 保留对此处任何产品进行更改的权利，恕不另行通知。

Freescale 对其产品在任何特定用途方面的适用性不做任何担保、表示或保证，也不承担因为应用程序或者使用产品或电路所产生的任何责任，明确拒绝承担包括但不局限于后果性的或附带性的损害在内的所有责任。 Freescale 的数据表和/或规格中所提供的“典型”参数在不同应用中可能并且确实不同，实际性能会随时间而有所变化。 所有运行参数，包括“经典值”在内，必须经由客户的技术专家对每个客户的应用程序进行验证。 Freescale 未转让与其专利权及其他权利相关的许可。 Freescale 销售产品时遵循以下网址中包含的标准销售条款和条件：freescale.com/SalesTermsandConditions.

Document Number AN4993
Revision 0, 08/2014