Freescale Semiconductor
White Paper

Document Number: KINETISMWP
Rev 0, 08/2013

Kinetis M Support for Distinct Separation of Legally Relevant Software

by: Joe Circello and Martin Mienkina

1 Introduction

We are surrounded by residential, commercial and light industrial electronic measuring instruments. Water meters, gas meters, heat meters, energy meters, weighing instruments, taximeters, and many more electronic measuring instruments are all around us. Currently, most of this equipment includes a microcontroller dealing with billing information and parameters that are subject to legal control. In other words, our bills depend on the accuracy and reliability of the measuring instrument and its control software. Both the International Organization of Legal Metrology (OIML) and European Cooperation in Legal Metrology (WELMEC) provide advisory guidelines for writing applications for software controlled measuring instruments, namely, rules for software separation [1][2]. This document describes the basics of software separation and shows the Freescale Kinetis M microcontroller family is well suited for measuring applications where achieving software separation brings technical advantages, reduces development cost, and accelerates time-to-market.

Contents

2 Basics of software separation

From an engineering perspective, the measuring instrument is controlled by legally relevant and legally non-relevant software applications (see Figure 1).

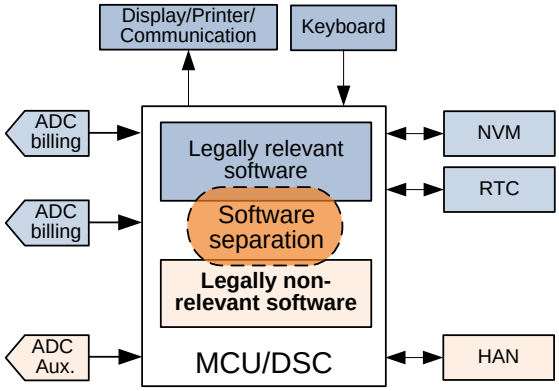

Figure 1. Measuring instrument software structure

Legally relevant application code ensures billing quantities are measured by analog-to-digital converters (ADCs), post-processed, displayed, printed, and transformed into encrypted data packets. This application also maintains billing information, log files, and load profiles in a Non-Volatile Memory (NVM). Certain information must be stored at predefined times, so operation of the Real-Time Clock (RTC) module is controlled by the legally relevant application.

Legally non-relevant applications perform all remaining software tasks including communicating digitally-signed packets to the utilities and providing data to equipment attached to a Home Area Network (HAN). For example, a washing machine equipped with a HAN communication interface can be programmed to start washing automatically during non-peak hours so that the consumer can take advantage of lower rates. Other smart appliances like electric heaters can be set to turn off/on automatically at specified times and thus manage the peak load. The size of legally non-relevant code in the metering instrument is increasing; the capability of a measuring instrument to share informative data using various protocols and formats with smart appliances is becoming crucial. If required functionality or protocol is not supported, then the manufacturer of the metering instrument has to make it available quickly and inexpensively.

As noted, only the legally relevant portion of the measuring instrument firmware is subject to legal control; after the relevant application is approved, the manufacturer cannot modify it without re-approval. If a software separation methodology is not implemented, then the entire firmware of the device is considered as legally relevant application and any modification requires a costly and time consuming re-approval. On the contrary, if a software separation methodology is implemented according to the OIML and WELMEC advisory guidelines, then manufacturers can modify the legally non-relevant application without re-approval, gaining flexibility, and significant cost savings.

The system architects at Freescale have dealt with hardware support for operating systems and software separation for more than two decades. More recently, microcontrollers have included a Memory Protection Unit (MPU) to protect accesses to on-chip and external memories. Freescale's Kinetis K

microcontrollers further extend memory protection by controlling accesses to the most of the on-chip peripherals. Undoubtedly, the new Kinetis M microcontroller series is the most advanced in terms of software separation. The system platform of Kinetis M devices has specifically been designed to provide hardware support for software separation. Besides hardware blocks dedicated to controlling accesses to on-chip memories, peripherals, and input-output ports, these new devices also integrate high performance analog peripherals, along with a variety of digital blocks and communication options.

3 Kinetis M microcontroller series

Freescale's Kinetis M microcontroller series has necessary on-chip peripherals, computation performance and power capabilities to enable development of low-cost and highly integrated metering instruments (see Figure 2). It is based on the 32-bit ARM® Cortex®-M0+ core with CPU clock rates up to 50 MHz. The Measurement Front-End is integrated on all devices; it includes a highly accurate 24-bit Sigma Delta ADC, Programmable Gain Amplifier (PGA), high precision internal 1.2 V Voltage Reference (VRef), Phase Shift Compensation block, 16-bit SAR ADC and Peripheral Crossbar (XBAR). The XBAR module acts as a programmable switch matrix allowing multiple simultaneous connections of internal and external signals. Accurate Independent Real Time Clock (IRTC) with passive and active tamper detection capability is also available on all devices.

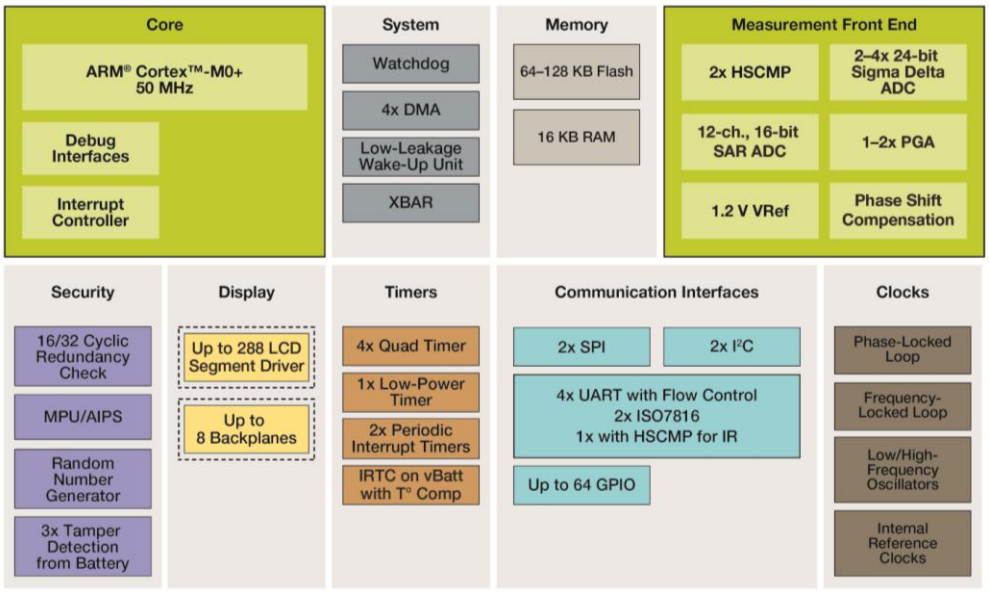

Figure 2. Kinetis M block diagram

In addition to high performance analog and digital blocks, the Kinetis M microcontroller series has been designed with an emphasis on achieving the required software separation. It integrates hardware blocks supporting distinct separation of the legally relevant software from other software functions. The hardware blocks controlling and/or checking the access attributes include:

- ARM Cortex-M0+ Core
- DMA Controller Module
- Miscellaneous Control Module
- Memory Protection Unit
- Peripheral Bridge
- General Purpose Input-Output Module

The Kinetis M System Platform supports two bus masters; the ARM Cortex-M0+ Core and DMA Controller Module (see Figure 3). The masters can be optionally enabled or forced by the Miscellaneous Control Module (MCM) to generate either User or Privileged access modes [3].

Besides traditional User or Privileged access modes, the device-specific Miscellaneous Control Module adds an access attribute indicating a Secure or Nonsecure state based on a software-controlled process identifier. Software or a DMA channel that executes in Privileged Secure access mode has no restrictions to the device resources. Conversely, software or a DMA access that executes in User Secure or Nonsecure access mode has lower priority than those executing in Privileged Secure mode. Also, software or DMA accesses that execute in User Secure or Nonsecure mode cannot access the core's System Control Block, Nested Vectored Interrupt Controller and System Timer. These basic User Secure or Nonsecure access mode restrictions are further extended by the platform to limit access to all on-chip peripherals that are critical to chip configuration, reset control, and power management. The result is a 3-state hardware-enforced access priority model where Privileged (Secure) > User Secure > User Nonsecure.

The Kinetis M DMA Controller has four independent DMA channels, each with a programmable Transfer Channel Descriptor to operate in Privileged Secure, User Secure or User Nonsecure mode. Accesses that are not allowed terminate the bus cycle with an error.

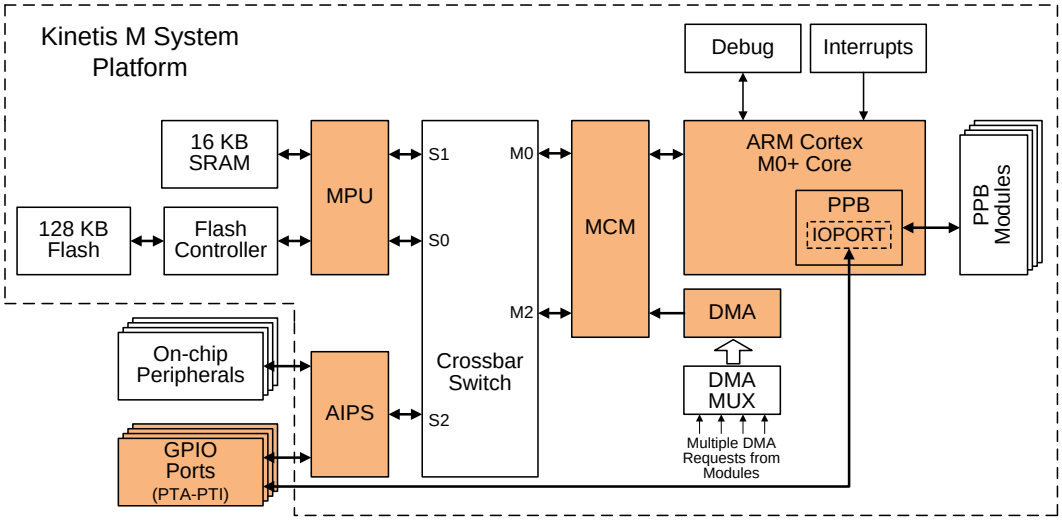

Figure 3. Hardware blocks with controlled access attributes

Following is the description of the hardware blocks that control access to on-chip memories and on-chip peripherals for the ARM Cortex-M0+ Core and DMA Controller bus masters using Privileged Secure, User Secure or User Nonsecure attributes.

First, the Memory Protection Unit provides hardware access control to on-chip flash and SRAM memories. It features eight programmable 128-bit region descriptors. Each descriptor defines start and end addresses and supports read, write and execute protection attributes for bus masters and access modes supported. This block detects access protection errors if a memory reference does not hit in any memory region, or if the reference is illegal in all hit memory regions. Accesses that are not allowed generate an error termination. The MPU is programmable only in Privileged access mode.

Second, the Peripheral Bridge (AIPS) converts the crossbar switch interface to a protocol compatible with the on-chip slave peripherals. It manages all bus master transactions ("bus cycles") destined for the attached slave devices and allows programmable unique access rights for each attached slave device. Each peripheral slot defines read and write protection attributes for bus masters and access modes supported by the module. Accesses that are not allowed generate an error termination. Like the MPU, the AIPS is programmable only in Privileged access mode.

Particular emphasis was given to access control support for the General Purpose Input/Output Module (GPIO). The Kinetis M microcontroller series has 68 GPIO pins grouped into nine ports. Each 8-pin port (PTA-PTI) supports read and write protection attributes for all bus masters and access modes supported by the port. The GPIOs are accessible through the Peripheral Bridge or IOPORT, a special single-cycle interface with the ARM Cortex-M0+ core. Illegal accesses through IOPORT are treated as RAZ/WI (Read As Zero/Write Ignored) while those through the Peripheral Bridge generate errors.

After any reset condition, including Power-on Reset (POR), the ARM Cortex-M0+ core starts executing software in Privileged Secure mode. It is necessary to initialize all discussed hardware blocks and program their associated access attributes. All configuration attributes can be locked by software until the next POR. After programming all access attributes, the measuring instrument firmware can initiate legally relevant and legally non-relevant software and DMA transfers. The more important legally relevant software tasks and DMA transfers execute in Privileged Secure access mode while less important legally non-relevant software and DMA transfers execute in User Secure or in User Nonsecure access mode to prevent their access to resources critical for device configuration as well as not to influence execution of the legally relevant software.

4 Conclusion

Since multiple semiconductor vendors produce microcontrollers with analog, digital and computational performance sufficient to realize single chip metering instruments, support of the OIML and WELMEC advisory guidelines for achieving software separation is becoming a prerequisite for conformity assessment of the product. Accordingly, these advisory guidelines are now considered as the best practices in microcontroller-based metering instrument design and followed by both manufacturers and certification bodies responsible for conformity assessment of the product.

Freescale’s Kinetis M microcontroller series has the right set of analog and digital on-chip peripherals to enable development of the low-cost and highly integrated metering instruments. Its rich peripheral set is well balanced with the ARM Cortex-M0+ core with CPU clock rates up to 50 MHz and low-power capabilities. In addition to the integrated peripherals, the Kinetis M microcontroller series has been designed with the hardware architecture to support software separation.

All these features along with low-cost and low-power capabilities of 90-nm process technology make the Kinetis M microcontroller series ideal for water meters, gas meters, heat meters, energy meters, weighing instruments, taximeters, and growing residential, commercial and light industrial electronic measuring instrument applications that are increasingly ubiquitous today and growing more capable in the future.

5 References

1. OIML, OIML D31, “General Requirements for Software Controlled Measuring Instruments”, edition 2008 (E), available at:
   http://workgroups.oiml.org/tcsc/tc-07/tc-07-sc-04/reference-documentation/D031-e08.pdf
2. WELMEC, WELMEC 7.2, “Software Guide (Measuring Instruments Directive 2004/22/EC)”, available at:
   www.welmec.org/fileadmin/user_files/publications/WELMEC_07.02_Issue5_SW_2012-03-19.pdf
3. ARM Cortex-M0+ Devices - Generic User Guide, 2012 ARM, available at:
   http://infocenter.arm.com/help/topic/com.arm.doc.dui0662b/DUI0662B_cortex_m0p_r0p1_dgug.pdf

6 About the authors

Joe Circello
Joe Circello is a Technical Fellow working as the core and platform chief architect in the Microcontroller Group at Freescale Semiconductor. In 22+ years at Motorola/Freescale, he has served as chief architect for the MC68060 and all ColdFire processors as well as a large variety of 32-bit platforms included in automotive, ColdFire and Kinetis microcontrollers. Joe holds 34 U.S. patents with 15 applications pending, and received a BSEE from the Milwaukee School of Engineering and an MSEE from Arizona State University.

Martin Mienkina
Martin Mienkina received the M.Sc. and Ph.D. degrees in electrical engineering from the University of Zilina in 1992 and 1997, respectively. Since 2000, Martin has been working in Freescale Czech System Centre (Roznov pR) firstly in the position of System Application Engineer and secondly as System Solution Engineer with the main focuses on the processors for electric drives, smart metering and new microcontroller definition and development.

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.

Document Number: KINETISMWP
Revision 0, 08/2013