Security in IoT Applications

Firmware Protection for XMC4000 Microcontrollers

By **ELE Times** - November 30, 2016

The outlook for IoT applications is impressive. The Internet of Things should make roughly a 15 trillion US dollar contribution to the global gross social product in the next twenty years (source: General Electric), with an installed base of 28.1 billion units by 2020 (source: IDC). But these figures are not only impressive, but simultaneously alarming when one considers the security aspects associated with the IoT revolution. It is important to take advantage of these developments while still ensuring both functional safety and data security. Security aspects affect all the systems involved, from PCs, IPCs, embedded systems, mobile devices, and PLCs to the microcontrollers used. Wibu-Systems, working with Infineon, has now introduced the CodeMeter µEmbedded, an efficient firmware protection for systems based on the XMC4000 microcontroller, in particular in applications such as IoT or Industry 4.0.

The "Internet of Things" (IoT), with its different variants such as Industry 4.0, information and communications technology, smart homes, and networked automobiles, requires a high level of security.

Figure 1: Networked systems in IoT designs have numerous points of exposure for attacks and manipulation. Secure firmware updates and functional extensions to microcontroller-based systems are a basic requirement for ensuring data security in IoT applications

Typical application cases include the authentication or licensing of components based on their unique identity, monitoring and securing system integrity, the protection of data and communications, as well as secure updates and upgrades. To build trust in new services and technologies, IP protection is also essential. Corresponding solution concepts require embedded system solutions based on secure hardware that protects the infrastructure and components from attacks, fraud, and sabotage. Since essentially all embedded systems integrated into IoT concepts are based on microcontrollers, this is the first level on which the corresponding protective functions must rely.

The general challenge in the implementation of maximum security in microcontroller applications lies in the fact that the solution must also be usable under harsh industrial conditions and easy to integrate. CodeMeterµEmbedded was developed based on the proven CodeMeter solution from Wibu-Systems for the protection, licensing, and security of systems. It particularly addresses the security aspects of firmware updates and functional extensions of microcontroller-based systems. The corresponding keywords here are code integrity, license monitoring, and protection from reverse engineering and copying of program code.

The implementation of CodeMeterµEmbedded was carried out in collaboration with Infineon and is based on the 32-bit microcontroller family XMC4000.

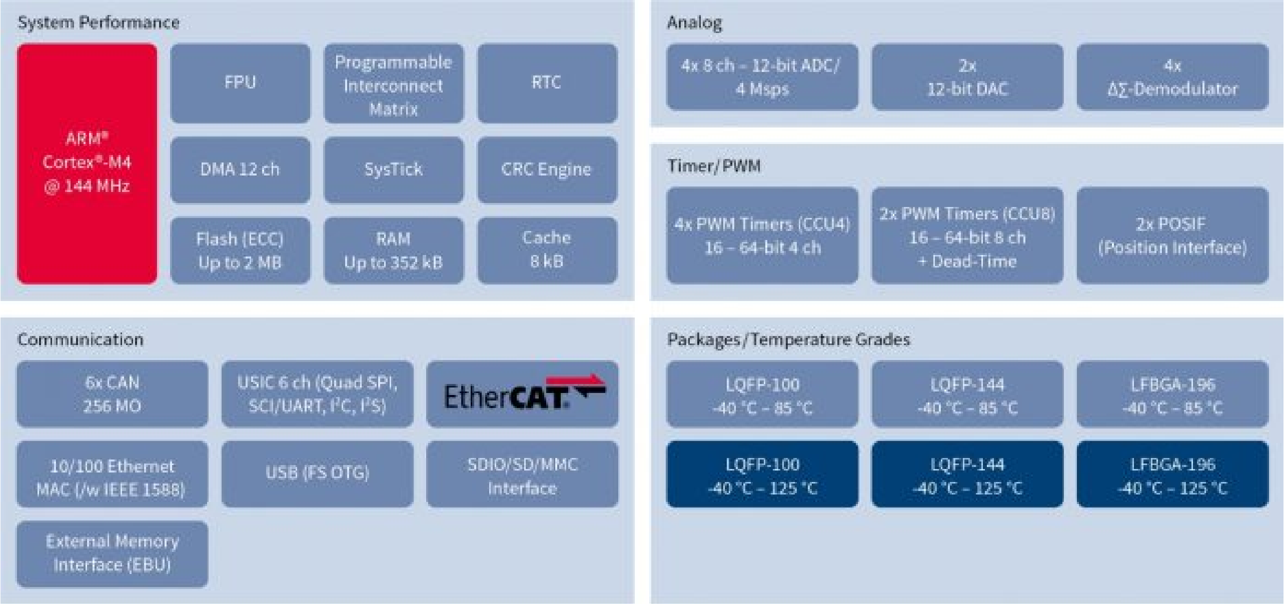

System Performance
ARM® Cortex®-M4 @ 144 MHz
FPU
Programmable Interconnect Matrix
RTC
DMA 12 ch
SysTick
CRC Engine
Flash (ECC) Up to 2 MB
RAM Up to 352 kB
Cache 8 kB
Analog
4x 8 ch – 12-bit ADC/ 4 Msps
2x 12-bit DAC
4x ΔΣ-Demodulator
Timer/PWM
4x PWM Timers (CCU4) 16 – 64-bit 4 ch
2x PWM Timers (CCU8) 16 – 64-bit 8 ch + Dead-Time
2x POSIF (Position Interface)
Communication
6x CAN 256 MO
USIC 6 ch (Quad SPI, SCI/UART, I²C, I²S)
EtherCAT
10/100 Ethernet MAC (/w IEEE 1588)
USB (FS OTG)
SDIO/SD/MMC Interface
External Memory Interface (EBU)
Packages/Temperature Grades
LQFP-100 -40 °C – 85 °C
LQFP-144 -40 °C – 85 °C
LFBGA-196 -40 °C – 85 °C
LQFP-100 -40 °C – 125 °C
LQFP-144 -40 °C – 125 °C
LFBGA-196 -40 °C – 125 °C

Figure 2: The 32-bit microcontrollers in the XMC4000 family offer appropriate performance and peripherals with powerful communications interfaces for use in IoT designs

CodeMeter µEmbedded extends the standard development tools to provide secure firmware updates and functional extensions in embedded systems based on the XMC4000.

Secure firmware updates and functional upgrades

Microcontrollers are increasingly used in frequently networked applications such as pumps, motor drives, sensors with field bus connections, and similar systems. In these applications, the secure loading of updates and/or functional upgrades is a significant security-critical aspect. The task of CodeMeter µEmbedded is to ensure secure loading of updates into the XMC4000 microcontroller and to introduce new functionality even in insecure environments. In highly networked and intelligent systems such as those in IoT, these important aspects must be considered:

- Only trustworthy code may be loaded into the controller. The code must be encrypted during transmission and loading. This is done using a unique key stored in the boot ROM of the controller.
- Traceable, reliable licensing must also be guaranteed while loading the code onto the controller. It should be possible to block or activate additional functionality of the microcontroller.
- The code may only be loaded and decrypted on authorized (licensed) controllers. It is essential to ensure that use on an unlicensed controller or emulator is prevented.

Integrated into the development environment

CodeMeterµEmbedded protects the firmware of the controller against manipulation, reverse engineering, and copying during updates. OEMs who develop software for controllers can also extend system functionality.

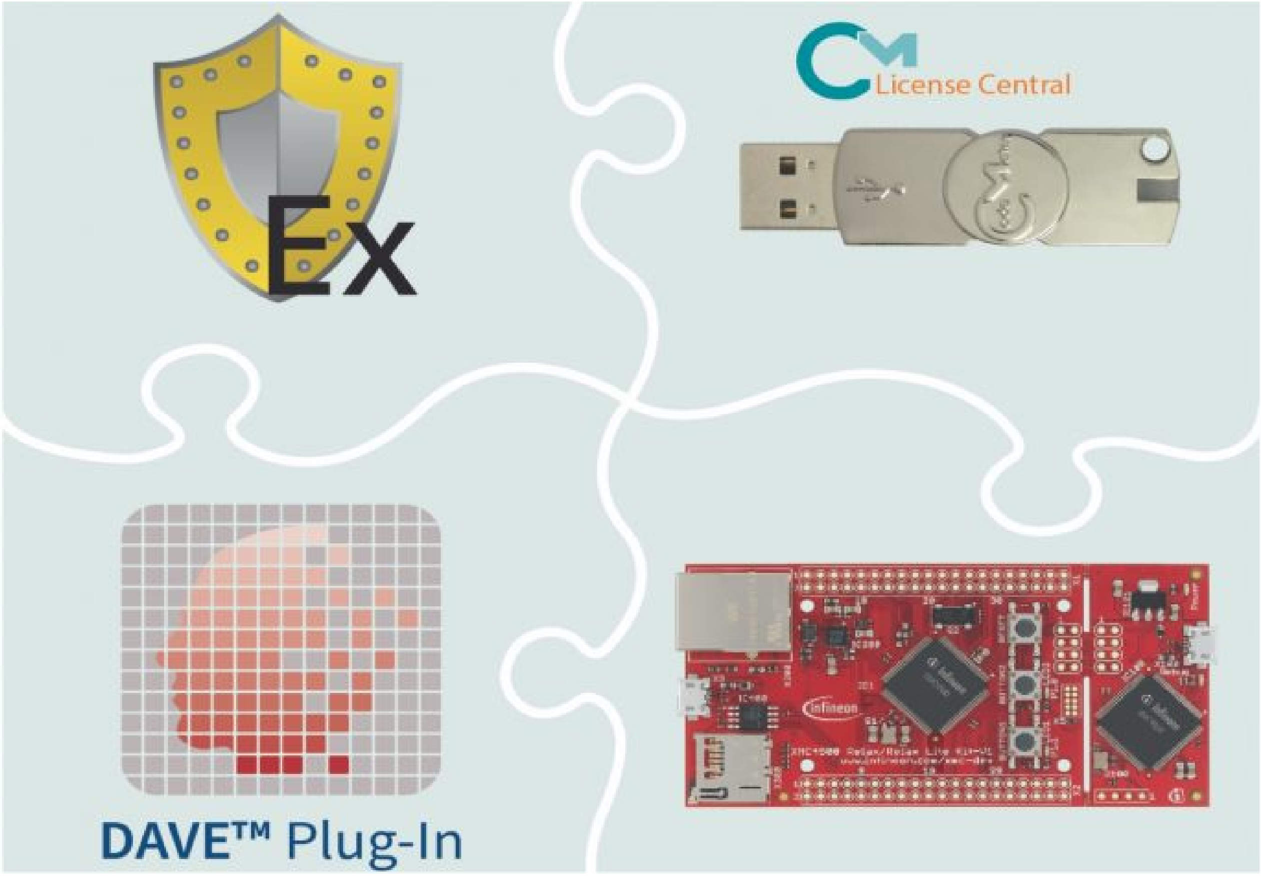
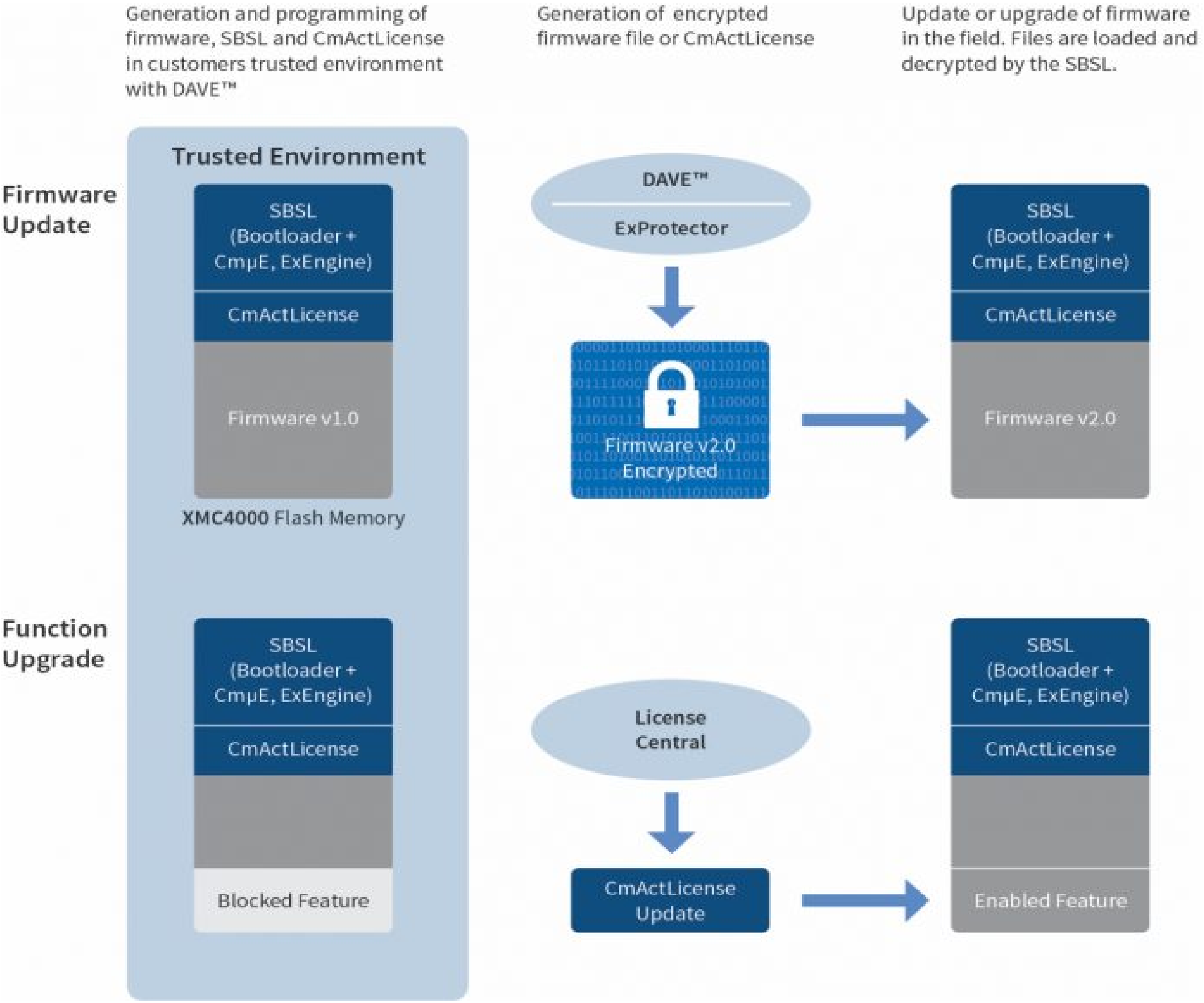


Figure 3: CodeMeterµEmbedded permits efficient firmware protection for systems based on XMC4000 microcontrollers. Secure functional upgrades to the XMC4000 microcontroller are also provided

The user can load a new encrypted firmware version from an external environment into the controller. This triggers encryption through the development environment – such as DAVE 4.0 from Infineon. Therefore, an appropriate plug-in is installed in DAVE.

DAVE Version 4 is available for download as a free development tool. This professional Eclipse-based development platform supports the user in developing software, from evaluation to final product. Among other things, an extensive peripheral- and application-oriented, component-based code repository is available. DAVE also generates appropriate code for the peripherals of XMC microcontrollers. With DAVE, the user can take advantage of commercial third-party tools for ARM to translate, link, and load the C source code configured and generated in DAVE onto the MCU. That covers the entire development cycle from evaluation to first prototype to final product, giving users maximum freedom in fast, efficient, platform-oriented software and product development.

After transfer to the XMC4000 microcontroller, the firmware is decrypted and stored in the flash memory. The XMC4000 handles the decoding. The microcontroller can generate a request with its unique “fingerprint” for later upgrades. This encrypted request is then transmitted to the manufacturer, who generates an appropriately licensed update and sends it back. The licensing update transmitted to the microcontroller can be used to provide new licenses or new functionality.



Generation and programming of firmware, SBSL and CmActLicense in customers trusted environment with DAVE™
Generation of encrypted firmware file or CmActLicense
Update or upgrade of firmware in the field. Files are loaded and decrypted by the SBSL.
Firmware Update
Trusted Environment
SBSL (Bootloader + CmμE, ExEngine)
CmActLicense
Firmware v1.0
XMC4000 Flash Memory
DAVE™
ExProtector
Firmware v2.0 Encrypted
SBSL (Bootloader + CmμE, ExEngine)
CmActLicense
Firmware v2.0
Function Upgrade
SBSL (Bootloader + CmμE, ExEngine)
CmActLicense
Blocked Feature
License Central
CmActLicense Update
SBSL (Bootloader + CmμE, ExEngine)
CmActLicense
Enabled Feature

Figure 4: Complete development environment with embedded security: A new plug-in for the DAVE development environment offers developers a simple graphical interface for configuring the XMC4000 microcontroller and generating encrypted firmware updates or license files.

The integration of this solution into DAVE as a plug-in (Figure 4) permits its use in a variety of application cases based on a technology or development environment with efficient firmware protection. Functional upgrades can be carried out without changes to the firmware, while secure firmware updates are possible even in insecure environments. The solution is also easy to handle and customer-friendly, while using the latest in encryption technology.

Protecting application code in microcontrollers

CodeMeterμEmbedded is a security variant specifically developed for Field Programmable Gate Arrays (FPGAs) and microcontrollers. The software is characterized by extremely small space requirements (footprint) of less than 60 kbytes. This was achieved by reducing the functional scope of the solution to the absolute minimum. The licenses generated are compatible with any CodeMeter variants. Each license is bound to a unique ID of the FPGS or microcontroller. Licenses can be activated in the production environment directly during production, or afterwards by file exchange in a “features on demand” system.