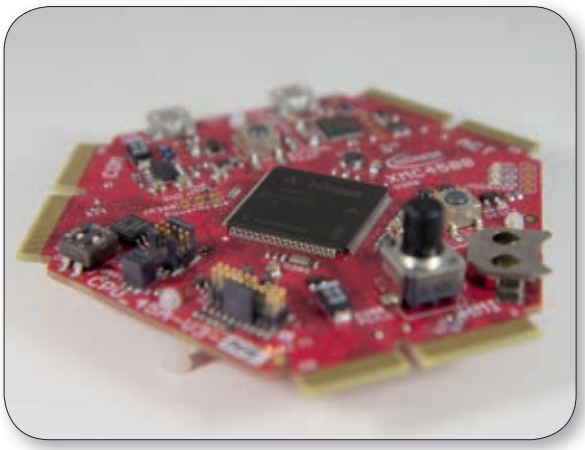
# Security for microcontrollers with IP protection and licensing

**By Marco Blume,** Wibu-Systems

*All products are designed to beat the competition. The effort that went into their development should pay off for as long as possible. This article explains how to shield microcontrollers with a level of protection on a par with larger systems – without having to dive into the depths of cryptography.*



■ Microcontrollers are all around us: digital watches at our wrists, smartphones in our pockets, tablets on our desks, light switches in our smart homes, and in the cars in our garage. Not to mention the clever little coffee maker on the countertop. Wherever we turn, we see devices that have long left the era of "on and off" switches behind. This has added so much comfort to our lives. Nowadays, watches can read emails, and air conditioning knows when we are in the room. Satnav systems knows where traffic is heaviest. Our smartphones know where we are heading, because our calendar is synced across all of our devices.

That is one side of the coin: the brave new comfortable world. There is another side we need to remember: the challenge of protecting our data, shielding our networks from attack, and not falling prey to software or hardware pirates. Just like a new home owner would never move in without locks installed on doors and windows, the design of intelligent devices also needs protection from the very start. But the entire package needs to fit – the most modern lock will not keep criminals out if the door itself is a thin sheet of plywood. This example should remind developers that they need to see security holistically in the design process to end up with a completely integrated solution against as many attacks as possible.

The level of protection depends on the quality of the measures taken and later compliance. This is where many developers enter unfamiliar terrain. Most are specialists in their areas and not experts for cryptography or secure software design. Users would ideally not be reminded of any security matters at all, and security must not hike up the costs.

The predictions for IoT applications are mind-bending: the IoT is expected to contribute around $15 trillion to global GDP in the next 20 years (source: General Electric), with 28.1 billion units installed by 2020 (source: IDC). These are not only impressive figures; they are also a wake-up call for the security issues created by the IoT revolution. Wibu-Systems has teamed up with Infineon to develop CodeMeter µEmbedded, an efficient firmware protection for systems using the XMC4000 microcontroller family, especially in the Industrial IoT. This article presents the integration on an XMC microcontroller as an example that can be adapted to nearly any other microcontroller platform. The functional principle stays the same.

The IoT comes in many shapes and sizes: Industrie 4.0 or smart homes and smart cars. What they all need is uncompromising security. Typical use cases include the authentication and licensing of components, monitoring and protection of system integrity, protection of data and communication channels, and the safety of upgrades and updates. This needs integrated solutions based on secure hardware to protect our infrastructure and its many components against attacks, fraud, and manipulation. Since all embedded systems used in the IoT are built around microcontrollers, this is the first line of defense.

The challenge for secure microcontrollers lies in making the chosen solution simple to integrate and usable even under tough industrial conditions. Wibu-Systems has developed CodeMeter µEmbedded based on its CodeMeter technology. The solution focuses on secure firmware updates and feature upgrades. Code integrity, license monitoring, protection against reverse engineering, and copy protection are key. Safety (for the user) is not an issue – the laws in this area are legion. Security (for the device) is, however, not guaranteed by similar legislation or universally accepted regulations. The CodeMeter µEmbedded use cases cover the most common security aspects. 1) Integrity protection: the microcontroller must only work with firmware from a defined source that must not be changed without proper authority. 2) IP protection: users in the field need to be able to load the firmware, so it needs to be protected against reverse engineering. 3) Licensing: there should be

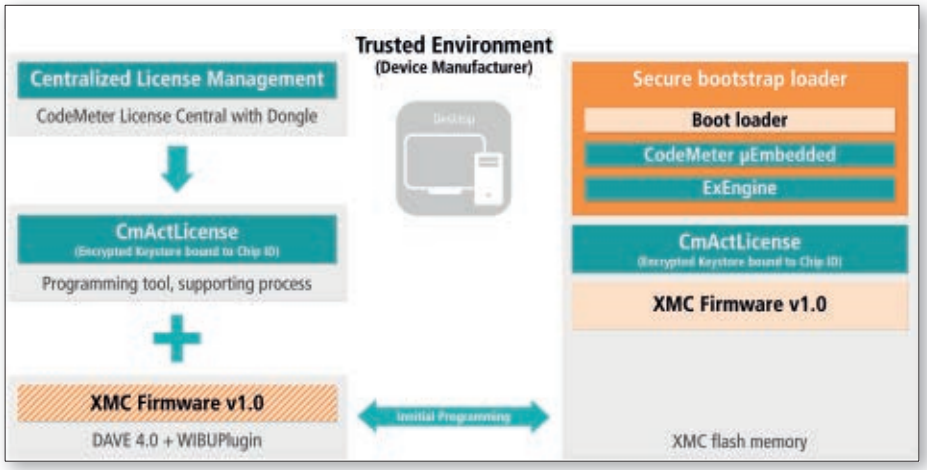



*Figure 1. The components involved at the developer and in the XMC controller*

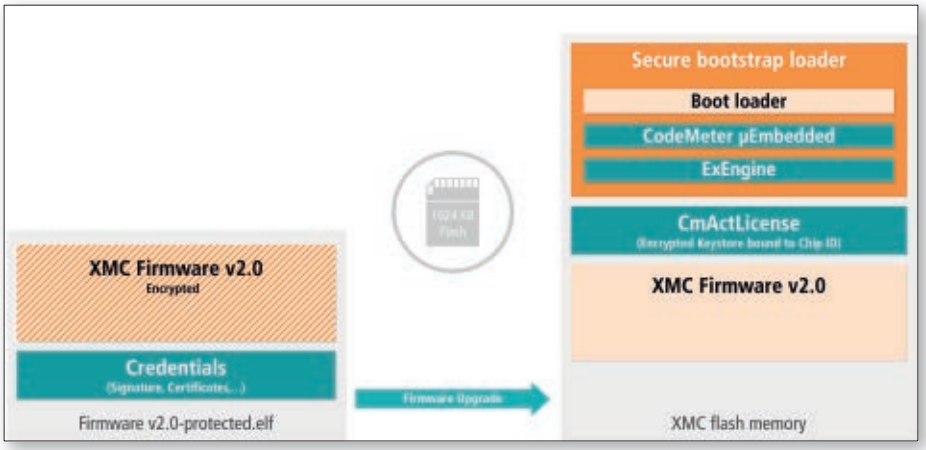



*Figure 2. Firmware is encrypted by the SBSL and remains in the XMC controller.*

an option to activate additional features via licenses upgrade without replacing the firmware in the field. In their mission to give developers an easy-to-use solution, Wibu-Systems and Infineon have pooled their resources in one package: Version 4 of DAVE development tool is available as a free download. The Eclipse-based platform makes software development easy with a vast periphery and application-oriented code repository. The. developer can use commercial third-party tools to translate the C source code for ARM and load it into the microcontroller. This covers the entire development cycle from first evaluation to the final product, while giving the developer maximum autonomy for fast and efficient platform-driven software and product development.

CodeMeter µEmbedded was developed specifically for microcontrollers and Field Programmable Gate Arrays (FPGAs). Larger systems like PLCs or PCs can use two other, fully compatible flavors of the technology: CodeMeter Embedded and CodeMeter Runtime. CodeMeter µEmbedded comes with a minimal footprint of less than 80 KByte, which was achieved by slimming the solution down to the minimum features for its intended use cases. The licenses are bound to the unique ID of the microcontroller and entitled during production. With the right license file, additional features can be activated in the field.

CodeMeter µEmbedded can also be used to store symmetric and asymmetric keys in protected memory. These keys can then only be used on devices with the right ID e.g. to check device licenses, track production volumes, or load encrypted application code onto the devices. The users benefit from the ability to use familiar tools like DAVE and CodeMeter Protection Suite, which handle all cryptographic operations. A new plug-in for DAVE gives the developers a neat interface to configure their XMC4000 microcontrollers and create encrypted firmware updates or license files.

The XMC4000 family of microcontrollers for industrial applications was made with digital power converters, electrical drives, and sensor devices in mind. All XMC4000 microcontrollers work at temperatures up to +125° C. They use ARM Cortex M4 processors with built-in DSP capabilities, floating point unit, direct memory access (DMA), and a memory protection unit (MPU). The extensive periphery includes analog/mixed-signal converters, high-resolution timers/PWM channels, and interfaces for all common industrial communication standards. The XMC4800 series comes with on-chip EtherCAT (Ethernet for Control Automation Technology) for simple and cost-efficient real-time Ethernet communication.

The solution is built on a secure bootstrap loader (SBSL) injected into the XMC controller during production. It accesses a CmActLicense bound to each controller that contains the keys to decrypt the firmware. After the SBSL and license are loaded, the controller switches into read-protected mode. Communication with the firmware only goes via the SBSL launched on start-up. The protection effort begins during the initial development at the OEM. The developers can use their accustomed tools and methods and create a firmware v1.0 in DAVE, which comes with a dedicated plug-in for ExProtector by Wibu-Systems.

DAVE also creates a project for the SBSL. The developer only needs to reserve memory on the dongle for the required keys, and the SBSL can be loaded directly into the XMC controller. This is the only time that the firmware developers have to concern themselves with the security solution. Even secure key storage is made easy: the keys are stored right on the dongle.

In the secure production environment, the XMC4000 is equipped with a secure boot loader. A license file is created and bound to the controller ID. The actual license is only produced and the firmware v.1.0 loaded onto the device at that point. This can be scripted for an automated process, as there is no difference to a regular industrialized firmware download. Alternatively, the DAVE plug-in can take care of all steps for manual trials or small-batch production.

**Use Case 1:** firmware update in the field. This use case protects the firmware against reverse engineering by only allowing the device to load firmware that has not been tampered with. The firmware is created in DAVE and automatically signed and encrypted with ExProtector. The protected file can be transferred to the user without other safeguards, since it cannot be decrypted or changed outside the XMC4000. Any manipulation would break the signature and prevent the secure boot loader from loading and decrypting the firmware. The process is only completed if the signature is correct and intact.

**Use Case 2:** feature upgrade in the field. This use case revolves around one universal firmware that users can upgrade with new

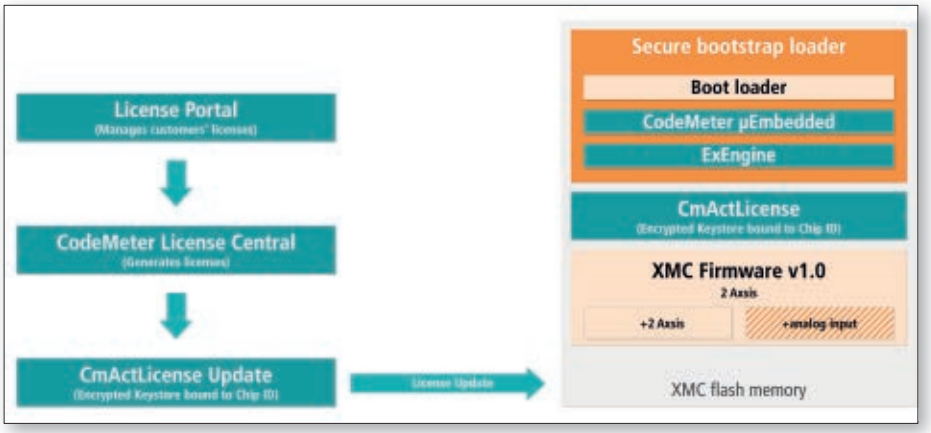



*Figure 3. The developer creates a license and upgrades features without changing the firmware.*

features in the field. The firmware itself is not replaced, not least to avoid costly testing and certification. The controller ID is ideally stored in CodeMeter License Central during development. The users can then buy new features from the device maker portal by entering their controller serial number. An encrypted license file is created for that system, where it e.g. activates additional movement patterns. Wibu-Systems offers a comprehensive package that makes it easier for developers to achieve powerful and flexible protection for their microcontrollers. No cryptography experts are required. Everything needed from encrypting software to managing licenses is already integrated and ready for use. Wibu-Systems offers the micro-embedded solution ready to use for Infineon XMC 4000. The package can be adapted and integrated for other platforms. ■