# IoT requirements for embedded system protection, licensing, and security

**By Oliver Winzenried,** WIBU

*More and more functions of IoT devices and machines are realized with software executed in embedded systems. This article introduces CodeMeter, a scalable solution that secures and monetizes any type of IoT software running on computers, embedded systems, and even small microcontrollers.*

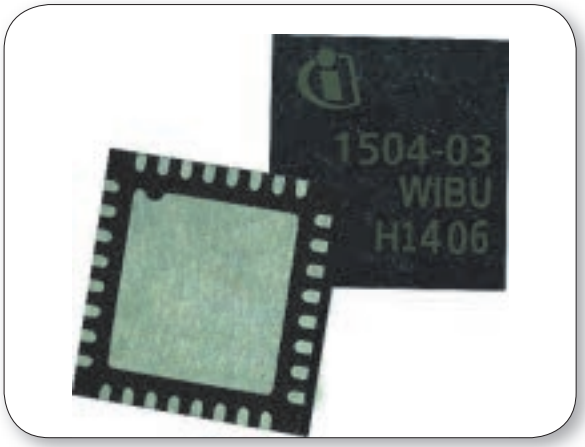


*Figure 1. CodeMeter ASIC in VQFN-32 package with USB and SPI interface and extended temperature range from -40°C…+105°C with integrated smart card chip and full CodeMeter functionality*

The Industrial Internet business has ignited a technological revolution and an economic renaissance that are advancing at an unprecedented pace. When the McKinsey Global Institute mapped out the real value beyond the hype, they estimated that the IoT has a total potential economic impact of USD 3.9 to 11.1 trillion a year. From a less visionary and more analytical approach, Ernst & Young has come to an additional observation: a combination of digital disruption and slow organic growth has propelled the global Tech M&A to a record second quarter in 2016, with deals worth more than USD 1 billion.

Analysts of Gartner Inc. estimate that 4.9 billion connected devices were in use at the end of 2015, which is 30 percent more than 2014. Five years from now, this is expected to rise to 25 billion devices. By then, the same analysts expect 10 billion connected devices (excluding PCs, smart phones and tablets) will ship each year.

These devices require protection against counterfeiting and product piracy, either in the form of simple 1:1 reproduction or, more specifically, in the form of reverse engineering, which remains the number one threat according to surveys done by the German Engineering Federation VDMA. Furthermore, secure licensing enables manufacturers to configure the features that can be executed individually per user. With simplified logistics, a larger number of devices with identical design can be produced; the units are then customized as the last manufacturing step, possibly even at the user side. By using standard hardware and software platforms, the time to market and development resources can be reduced. By the same token, new business models can also be introduced, such as pay-per-use or subscription models that create recurring revenue streams for device makers, instead of simple one-time sales. With a form of app store, additional features can be offered and more after-sales business can be created, as is already done with consumer smart phones. Additionally, security is getting top priority, as increasing connectivity is increasing the risk of attacks. Secure firmware updates, secure identities, and key storage are required for the protection of code, parameters, and data.

While protection solutions for applications running on standard computers have been in the market for almost three decades, the different nature of embedded systems requires a different approach. They are using a variety of embedded and real-time operating systems, they are often limited in terms of system resources like RAM and storage space, and they are using different low-power CPU platforms, like ARM, PPC, or X86.

CodeMeter is the universal technology for software publishers and intelligent device manufacturers, upon which all other solutions from Wibu-Systems are built. It offers protection, licensing, and security capabilities. It needs to be integrated into established software or business workflows at a single point in time only. Applications and libraries can be encrypted and signed with Protection Suite. In addition, CodeMeter offers an API for custom integration, and CodeMeter License Central can be connected to existing ERP, CRM, and e-commerce systems. Once integrated, manufacturers can create licenses automatically and deploy them seamlessly to connected target systems or distribute them via a separate license portal. Essentially, each user or device receives the same software, but a different license that entitles them to use the product in a tailor-made way for their needs.

CodeMeter offers maximum flexibility in how licenses are stored. CmActLicense stores licenses in an encrypted and signed file, bound to a fingerprint of the target system or to any type of secure element like TPM or technologies like Intel SGX or ARM Trustzone. CmDongles store licenses in a highly secure fashion in a smart card chip. The secret keys never leavethis chip. These CmDongles are available in a chip size package with SPI and USB interface, as USB devices, microSD

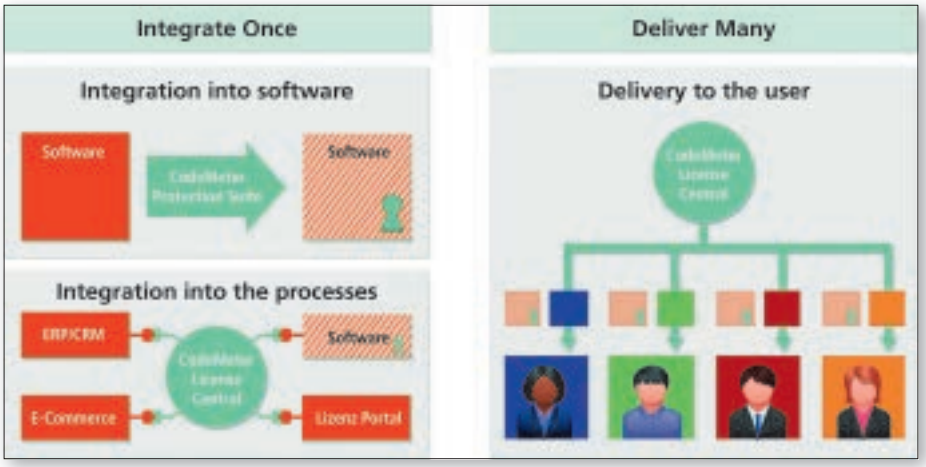


*Figure 2. One-time integration into software and business processes and multiple delivery*

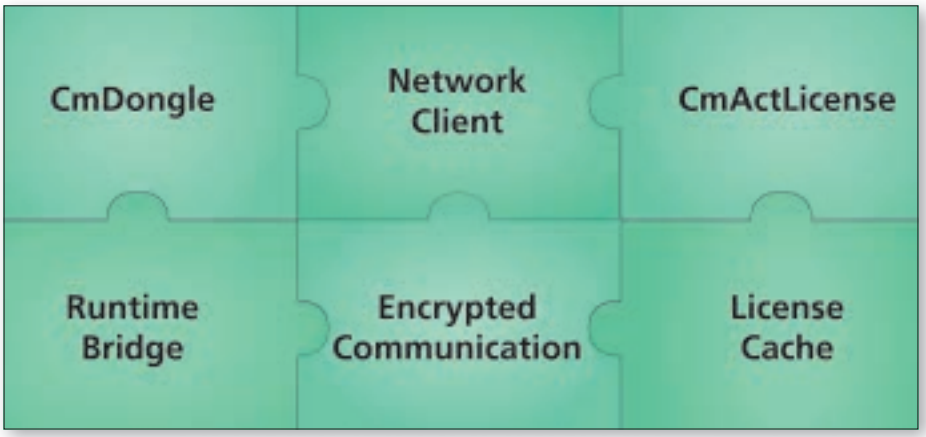


*Figure 3. CmEmbedded modules can be chosen by OEMs to tailor their perfect solutions*

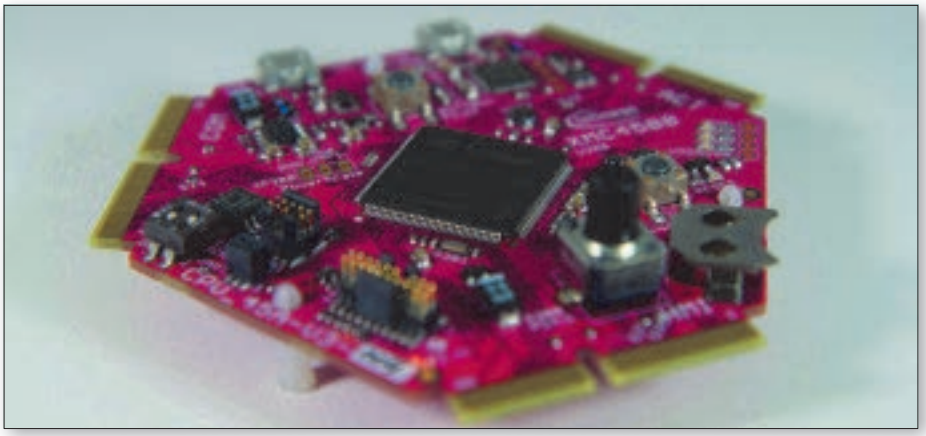

*Figure 4. Infineon XMC4500 development board with CodeMeter µEmbedded*

cards, SD cards, CF, or CFastcards. The cards offer additional industrial-grade flash memory in the same device.

To be able to use CodeMeter technology on any kind of system, the so-called CodeMeter Runtime is required. It offers access to the CodeMeter licenses and keys for the applications executed on the target system. Several different runtime versions are available. CodeMeter Runtime is intended to be used on servers, PCs, IPCs, and powerful embedded systems. It offers maximum functionality, e.g. including an integrated network license server and a web administration front-end, and is available as a ready-to-use installation package for all Windows variants, Linux, and macOS. It requires 10...30 MByte of RAM.

CodeMeter Embedded is intended for systems from IPCs, PLCs, and embedded systems down to powerful microcontrollers. It is available in the form of libraries and shared objects for many embedded OS, like Windows, Linux, Android, VxWorks, and QNX for Intel, PPC, and ARM processor platforms. It is also

on offer in Ansi-C source code for portability to any OS and any platform. It contains different modules for tailoring to the OEM's system requirements with the lowest possible footprint. The available modules are as follows.

CmDongles: this module allows the use of CodeMeter smart card hardware as a safe repository for keys and licenses. It can be tailored to support CmSticks with a USB connector (with and without flash memory), CmCards for microSD, SD, CF, and CFast interface that contain additional industrial flash memory, and CmASIC, the chip in a small VQFN package that can be connected via a USB or SPI interface.

CmActLicenses: this module allows the use of a CodeMeter via binding to specific properties of an embedded device. The OEM defines the type of binding for the device in question by using a specific adapter. Support for TEE, Trustzone, and SGX or secure elements like TPM (OPTIGA or Iridium) is an option for secure binding.

Network Client: this module allows access to licenses on a network server using TCP communication. Runtime Bridge ensures that the software compiled with CodeMeter Embedded integrated detects when a CodeMeter runtime is active on a target system and automatically uses this for communication.

Encrypted Communication: this module enables encrypted communication between CmDongles and protected applications using CmEmbedded. License Cache: this module holds information about available licenses in memory to give faster access to them and allow multiple processes to access licenses. All keys and encrypted data, e.g. hidden data, never need to leave the CmDongle or CmAct License.

CodeMeter µEmbedded is the variant made especially for field programmable gate arrays (FPGAs) and microcontrollers. It is characterized by an extremely small footprint for the loader code, amounting to less than 60 kBytes. This code contains the entire handling of CmAct Licenses, including transfers, symmetric and asymmetric cryptography, and a subset of the CodeMeter API. Within another about 16kByte of nonvolatile memory, CodeMeter µEmbedded can store up to 30 licenses, each from two different vendors. Only a few kByte of RAM are required. The licenses generated are fully compatible with all variants and can all be handled by CodeMeter License Central. The license is bound to a unique ID of the FPGA or microcontroller. Licenses can be activated directly in a production environment during manufacturing itself. In addition, features-on-demand can be enabled later via remote file update. Transferable licenses can be moved from a CmDongle or a CmAct License onto a device. Furthermore, with CodeMeter µEmbedded, the application firmware is protected by strong encryption and cannot be read by external devices trying to copy the firmware. The symmetric and asymmetric keys as well as the secure loader are located in a protected memory area of the target controller and can only be used on the device with a matching ID. The code size of CodeMeter Embedded ranges from 150 to 350 kByte depending on the CPU platform and the chosen modules and 500 kByte of RAM depending on the cache size for license information from the CmDongle or CmAct License. CodeMeter µEmbedded has been successfully integrated with the XMC4000 Infineon microcontroller family. Developers can protect their code against piracy and license their applications. The tools for the protection of the application code are fully integrated in the development platform DAVE. Typical use cases of CodeMeter µEmbedded are: license for devices and device functionality (microcontrollers and FPGAs), monitoring of production volumes through the licensing of individual devices, and secure encrypted transmission of application code into devices.

IoT devices require protection and licensing mechanisms that can be implemented in limited-footprint embedded systems just as much as in cloud-based license deployment solutions. Powerful protection tools enable IoT device developers to implement these complex cryptographic processes in an easy and fast process. The fully scalable runtime variants of CodeMeter fit any type of target system. CodeMeter Embedded is a market-proven solution used in PLCs from B&R, Codesys, and Rockwell Automation, in DAVE microcontroller development tools, in Wind Rivers VxWorks and Workbench, and many other scenarios. ■