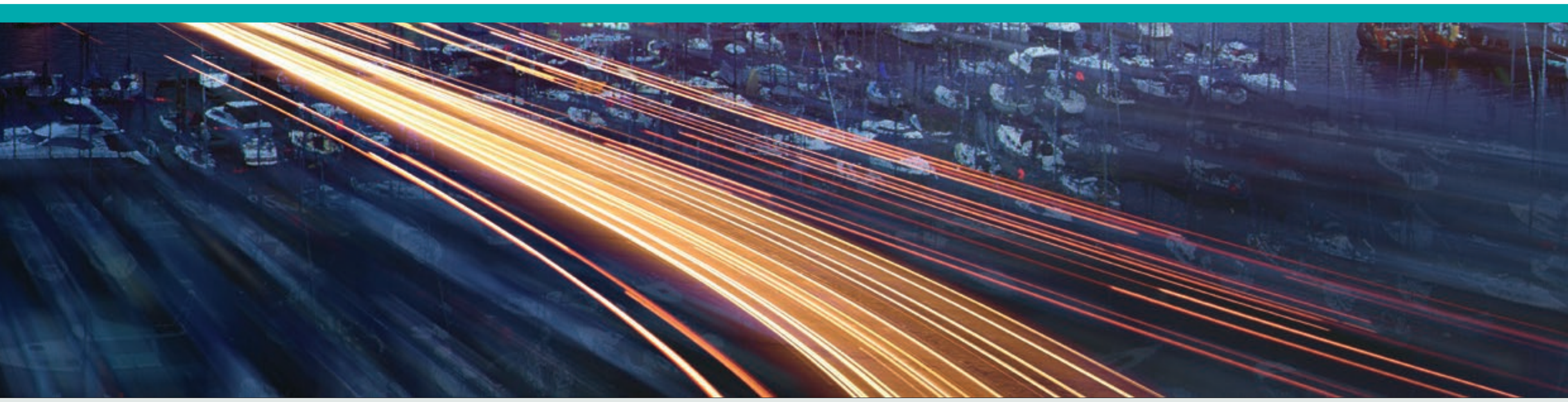
White Paper

Licensing and Security for the Internet of Things



Oliver Winzenried, CEO Wibu-Systems
www.wibu.com

WIBU SYSTEMS

Content

Autor:

Oliver Winzenried is a security enthusiast with a vocation to expand universal knowledge and apply innovative technologies to protect the intellectual property and business revenues of ISVs. With a degree in Electrical Engineering from the University in Karlsruhe, he began his entrepreneurial career immediately after completing his studies, and focused on electronic and ASIC design, hardware, microcontroller and embedded application development for consumer electronics, automotive and industrial engineering. With Marcellus Buchheit at his side, he then founded Wibu-Systems in 1989, and remains the company's CEO. His passion for software protection has resulted in numerous patents covering areas from secure license management and anti-tampering solutions to dongle feature innovations. He's also a prolific author, greatly contributing to editorials and books on the one hand, as well as addressing large audiences at trade shows, conferences, industry associations and technology centers like the Fraunhofer Institute. He is personally committed to R&D projects and organizations for standardization, such as the SD Card Association. Oliver Winzenried is also serving as chairman of the Product and Know-how Protection "Protect-Ing" committee of VDMA, member of the board of directors of Bitkom, and member of the managing board of the FZI at KIT. In 2015, he has been elected Manager of the Year in the Automation category by the readers of the German electronics publication Markt&Technik.

Many Names, One Idea

The Internet of Things (IoT), the Industrial Internet of Things, Industrie 4.0, Made in China 2025, Smart Industry, Connected Systems, Cyber-Physical Systems (CPS), Mobile Cyber-Physical Systems: many new phrases have been coined to describe something that is on everybody's mind, and that will influence our lives, our way of working, our future. What does the IoT mean for mechanical engineers or the manufacturers of controllers or other devices? This paper investigates the opportunities that lie ahead and the risks that await. Above all, it looks at which decisions can be made in order to become a successful player in the new world. For this paper, the term 'IoT' will stand for all of the many concepts named above.

Internet of Things (IoT)

Believe the Hype!

Nations around the world have come to consider the technical promises of the IoT as their future and have begun to invest heavily in research in the field, making IoT part of their long-term strategy. In the United States, the talk is of connected systems and researchers are concentrating on cyber-physical systems. China does not want to continue to be the world's factory for cheap mass produced goods, but rather become a leading industrial nation with home-grown high-quality offerings. The German idea of the Industrie 4.0 has inspired Chinese planners to draft the strategy paper "Made in China 2025". Simple maintenance, preemptive service planning, and client-specific, cost-efficient custom production are just some of the many advantages promised by the industrial IoT. The increasing pressure for cost reduction alone is powering the trend towards the IoT. Its market is expected to amount to approximately $1.8 trillion in 2020.

Focusing on Industry

IoT applications are developed with devices and services in various sectors: Information technology, automation and production technology, the aerospace industry, maritime and naval applications, railways, car makers and their suppliers, energy providers, agricultural businesses, medical technology, and building automation. These many and diverse areas share certain industrial-grade standards in terms of a technology's long life, reliability, robustness in harsh environments, or reliable, long term availability.

From Embedded Systems to the IoT

Embedded systems "see" with cameras, "feel" with pressure sensors, and "orient" themselves with GPS modules. They interact with the world around them and make decisions autonomously. Connected systems often include components that are located remotely and rely on networks to communicate. But more and more voices joining the conversation also means more and more potential victims for manipulation.

IoT is Here

In car factories, driverless transporters bring half-finished goods from production line to production line, where robots choose the tools they need from their kits to process the items at hand. All of this happens in mostly closed systems, relying on costly production assets.

IoT for a “Mission Possible”

IoT systems will complete old tasks in completely new ways and cope easily with challenges that previously seemed impossible. The vast expanse of the deep sea will be explored, robots will be sent to fight fires in places too dangerous for humans, robots will rescue lives, clear mines, provide care, nurture and grow plants and feed animals with their sensors to guide them. The list of activities that are suited for the IoT is already long and is growing every day.

Free Access and Its Enemies

The IoT systems of the future will rely on public networks, but public networks are not safe environments. Hackers are always looking for backdoors and exploits for their criminal plans. Attackers are trying to tamper with data to cause untold damage. The IoT has many unprotected flanks, which means that every component needs to have its own appropriate safeguards. Bitkom, ZVEI, and VDMA have worked together on a reference architecture, RAMI 4.0, which uses only fully secure and reliable channels of communication for components in factories to communicate with each other. That means that devices and functions are only cleared for operation after successful authentication and proven legitimacy.

Trends in IoT

1. IoT leaves the safety of closed systems

IoT in its infancy was mostly restricted to closed systems and capital equipment with long life expectancy, but it is now moving into all aspects of our lives. It will change our manufacturing methods and become ubiquitous even for fast-moving consumer goods. Remote maintenance, remote operations, remote monitoring, and remote management are already an everyday reality via the Internet. IoT reduces costs and makes business processes much simpler.

2. The USP of hardware will depend much more on software

Computing hardware and operating systems are becoming increasingly standardized. What differentiates one piece of equipment from the next is the applications running on it. Security embedded directly into the device guarantees the integrity of these applications and protects against reverse engineering, product piracy, and tampering.

3. New business models are evolving

Software-based functions can be brought to market as extra or after-sales options by means of license activation. Paid upgrades, pay-to-use features, or time and volume-controlled operations protect the commercial success of equipment manufacturers. The more versatile the licensing options, the more flexible the marketization opportunities. Licenses and manageable rights guarantee business continuity, but only if the relevant logistics are transparently integrated into the OEM’s and the end users processes.

4. Multiple manufacturers equip single systems

The components of diverse manufacturers and brands and software from diverse sources can come together in a single device. Post-hoc expansions or additions keep the system flexible and evolving.

5. New use cases and services

More and more devices will use the IoT for networking. In mobile cyber-physical systems, embedded systems work together in mobile devices of any size – from cars to smartphones – to form giant “neural landscapes”. New applications will evolve to take advantage of this evolving connectivity.

6. Simple components deserve protection

Comprehensive protection covers all parts of any system, including miniature components and devices with minimal storage space or computing power.

Strategies for Success

In the IoT, success depends not only on good products, good marketing, and good sales activities, but must include security, integrity, and reliable licensing.

Success Factors

- Additional revenue streams with licensing (optional features)
- New applications with rights management (servicing)
- Protection against reverse engineering, cloning, and copying (product piracy)
- Integrity preservation of communication (tampering)
- Integrity security for components by design (product piracy and tampering)

Standards for Protection and Licensing Systems in the IoT

In the IoT, security by design needs to be the goal for all components. This places a priority on industrial-grade design, the footprint of hardware and software, development support, and cross-brand cooperation as well as complete protection from the very first software layer. IoT-capable protection need to be physically and functionally scalable.

Integration in devices and software

- Device-oriented licensing
- Integration on many platforms / multi-platform support
- End-to-end ready-to-use protection and licensing from product development to operations and maintenance
- Industrial-grade properties
- Support for OPC UA
- Secure boot

Upgrades and updates

- Secure updates
- Licensable upgrades / Upgradability for network development

Licensing models

- Models tailored to the IoT

License management, access rights, and certificates

- Simple integration in all business processes, from development and production to sales and servicing
- License management in the cloud, with 24/7 self-service capabilities, including license activation and returns, transfer to other devices, upgrades, license renewal or cancellation.

Scalable safeguards

- Flexible pricing and service packages for different use cases
- Complete hardware, software, and cloud-based solutions
- Industrial-grade dongles in common form factors

Protection

- Data integrity
- Proof of origin
- Tampering protection
- Protection against reverse engineering, copying, or cloning
- Access rights

CodeMeter – The Industry and IoT-Ready Package

Wibu-Systems offers CodeMeter®, a complete package for protection, licensing, and security that fulfills all of these standards and requirements. The consistent and interoperable solution is fully scalable to match any job and application.

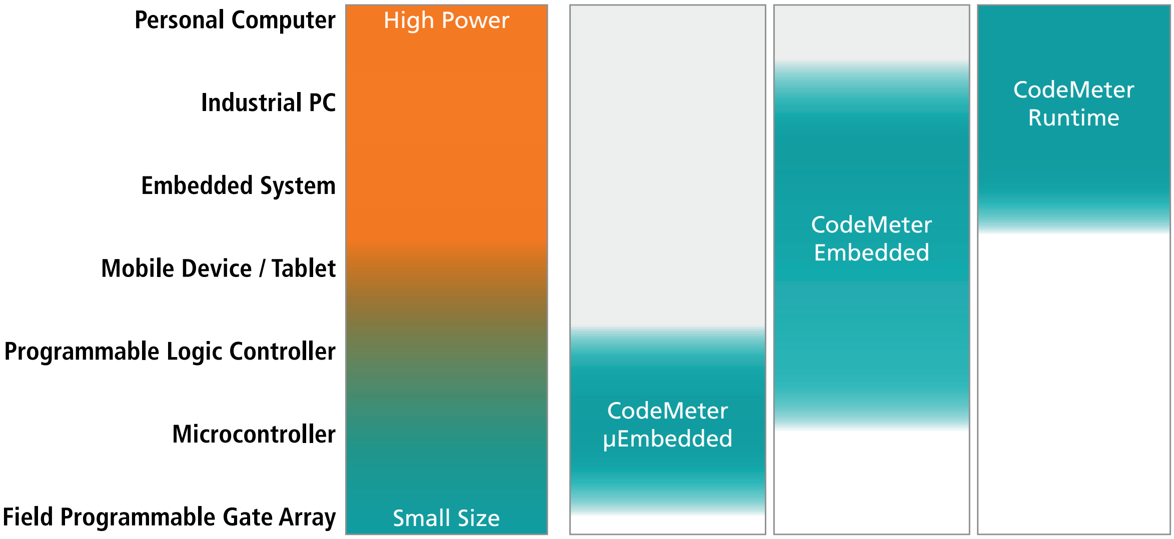
Software Integration
CM
Back Office Integration

Wibu-Systems Protection Concept

- CodeMeter
  - Licensing models with secure key storage
  - CodeMeter Runtime, Embedded, or µEmbedded
- Integration in Software
  - Automatic encryption
  - API queries
- Integration in Processes
  - ERP / e-commerce / MES / CRM
  - Online activation server

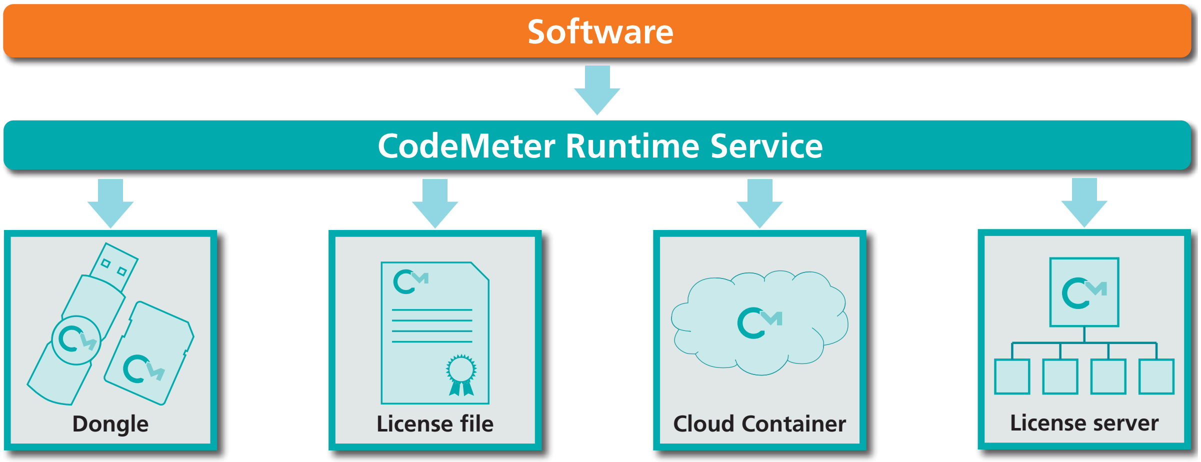
CodeMeter is the core product, available either as a dongle (CmDongle), device-bound license (CmActLicense), or cloud license (CmCloudLicense). CodeMeter's components are integrated in the protected software and via the back-office system into the processes.

CmDongle, CmActLicense, and CmCloudLicense are fully compatible and can be mixed and matched freely. The dongle offers the strongest and most flexible protection: When the device is replaced, CmDongle carries the licenses, rights, and certificates to the new device without any updates required. CmActLicense is the cost-efficient option.



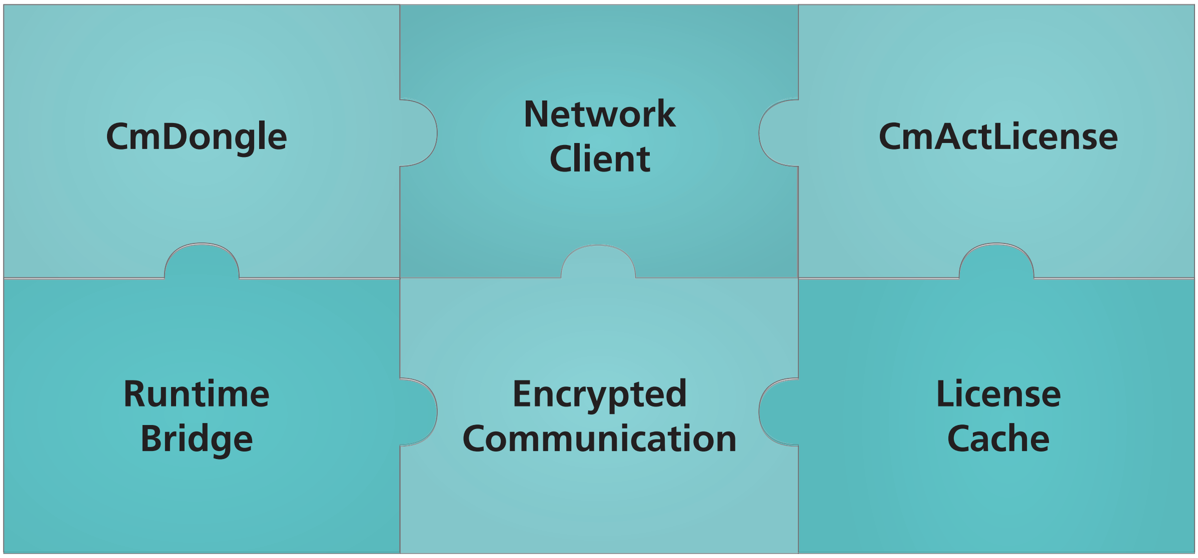
CodeMeter Runtime

CodeMeter Runtime is the perfect choice for standard PCs with operating systems like Windows, Linux, or OS X. It includes the network license server and prevents illicit use of licenses by virtual machines or terminal servers, while also tracking the license's use for statistical monitoring.



CodeMeter Embedded

CodeMeter Embedded was designed for embedded systems and IoT devices. It consists of multiple modules and is tailored to the needs of the equipment manufacturer. The code is very compact and ready for use even on systems with very limited resources. Its availability as source code enables CodeMeter Embedded for use on virtually all platforms.



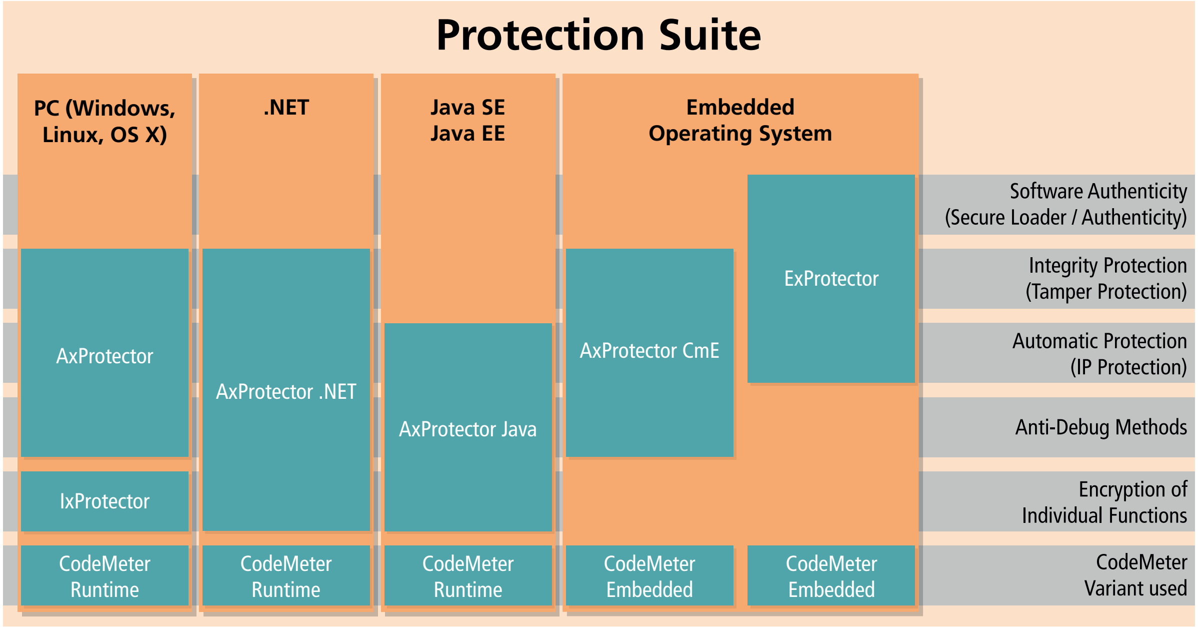
CodeMeter µEmbedded

Weighing in at less than 64 kByte, CodeMeter Embedded is a tiny package with a big punch. It was developed for the XMC4000 in cooperation with Infineon Technologies and is microcontroller-ready. The protection are tied to the chip's serial number at a very deep level of the hardware.

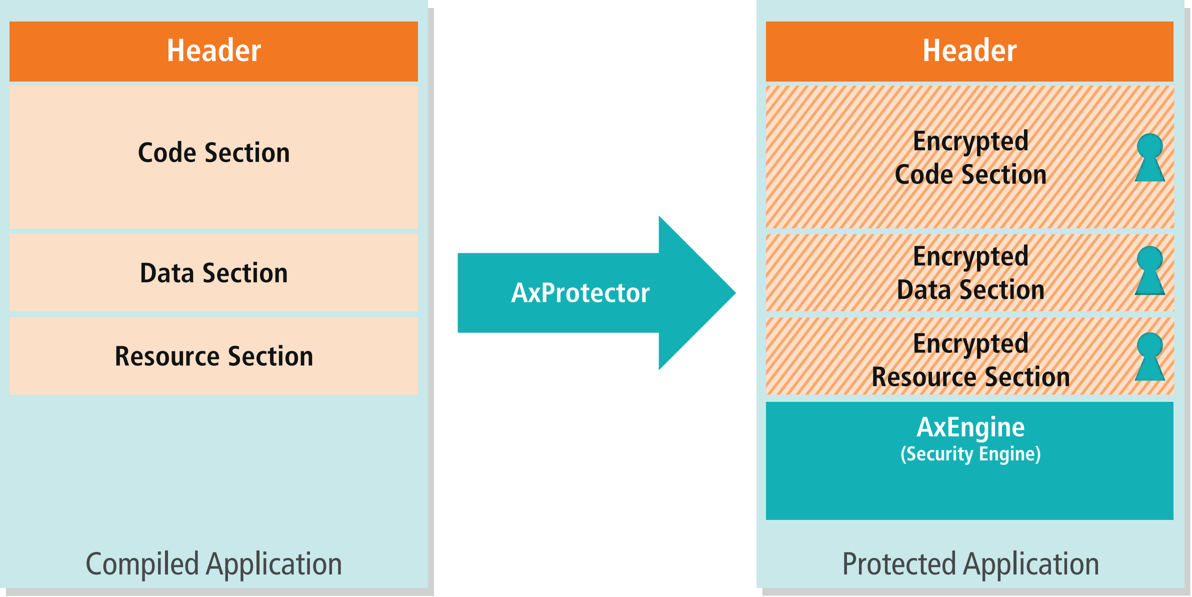
Licenses are fully interoperable between CodeMeter Runtime, CodeMeter Embedded, and µEmbedded. CodeMeter Runtime and CodeMeter Embedded contain all licensing options, while CodeMeter µEmbedded offers a specially chosen subset.

Getting the Protection onto the Device

The important decisions for security-by-design are made during development.

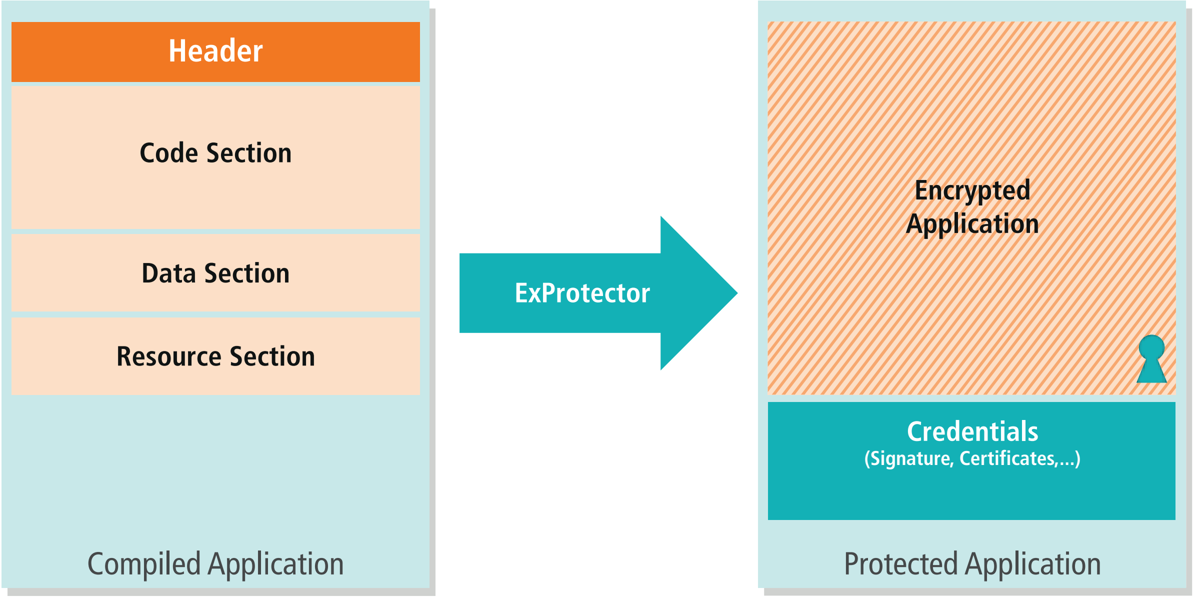


The protection are integrated with the tool Protection Suite and Wibu-Systems' CodeMeter API. Developers of microcontroller applications and embedded PCs can use programming languages like C/C++ to integrate CodeMeter with CodeMeter API. Protection Suite encrypts the software and comes in two basic flavors: AxProtector and ExProtector. AxProtector is used on standard operating systems like Linux, Android, Windows, or OS X. ExProtector is used on devices whose operating systems are customized by the device manufacturers, which is often the case with VxWorks and Linux. The architecture of ExProtector includes additional options for securing the integrity of the device and the authenticity of the application.



Built-In Authenticity with ExProtector

In the embedded world, OEMs distribute their devices with pre-configured operating systems. The application software is known, and software from unknown sources is unable to run on the device. Using ExProtector, software can be signed and encrypted, and parts of ExProtector (ExEngine) are built right into the operating system. The device itself sees whether an application comes from a legitimate source. ExProtector is standard for Linux and VxWorks and can be custom-tailored to QNX and Android.



CODESYS

Controller applications are developed by means of an IEC-61131 language. Integrating C-Code is often difficult, if not impossible. Protection and licensing usually needs the help of the controller's manufacturer to be implemented in the application software. Wibu-Systems has formed a strategic partnership with 3S-Smart Software Solutions GmbH, the maker of the Soft-SPS CODESYS. Controllers using CODESYS software already comes with Wibu-Systems protection on board. Application software and project files can be encrypted and secured with CodeMeter. A standard component of CODESYS allows licenses to be checked by the application code.

The runtime environment of CODESYS can check licenses and decrypt the protected software when the controller is activated.

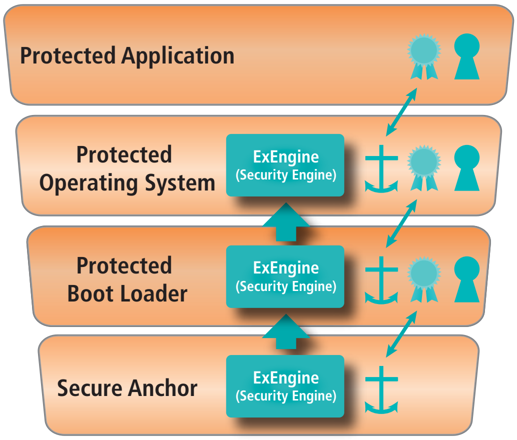
VxWorks 7®, Real-Time Operating System with Embedded CodeMeter Security

CodeMeter is an integral part of the Security Profile for VxWorks; its complementary extension CodeMeter Security is a hardware-based add-on to this real-time OS. Together, the two products represent a significant milestone for the whole community of VxWorks users who can now avail themselves of advanced and deeply entrenched security tools, in a time when IoT demands countermeasures against cyber-attacks on devices, machines, and facilities.

CodeMeter components were already available for earlier versions of the widely used real-time operating system from Wind River. With the latest Security Profile for VxWorks 7, developers of VxWorks applications can easily implement integrity, authenticity, and IP protection as well as certificate management. By upgrading to CodeMeter Security, intelligent device manufacturers can also extend these solid foundations of security with additional functions, such as copy protection, license management, and hardware-based key storage. The combined use of CmDongles and CodeMeter License Central with VxWorks opens new business opportunities to the embedded world that can now rethink its revenue models and offer, for instance, leasing or pay-per-use schemes. The system also represents a turnkey solution for controlling production volumes against product counterfeiting.

Secure Boot – Security by Design

A part of the boot loader is securely embedded in the system and cannot be replaced. This is the foundation for a secure process: Secure boot builds each protected step on another protected step. The actual boot loader is encrypted as are the operating system and the application. Each previous layer decrypts the next and checks whether it includes the right certificate. CodeMeter includes both the hardware and the software. The CodeMeter software can be bound to a CmDongle, the TPM chip, or another component to form this secure chain of checks and counterchecks.


Protected Application
Protected Operating System
ExEngine (Security Engine)
Protected Boot Loader
ExEngine (Security Engine)
Secure Anchor
ExEngine (Security Engine)

Industry-Grade Designs

CodeMeter's hardware offers top level protection, can store licenses, and comes with industrial-grade specifications. This includes support for wide temperature ranges from -25°C to +85°C, or even -40°C to +105°C in select products. The integrated flash memory uses Single Level Cell (SLC) technology for long life, low power consumption, and lasting availability. CodeMeter also protects its memory with AES encryption, making it industrial ready.

Hardware

CmDongles are available in all common form factors (USB sticks, microSD, SD, CF and CFast cards), built to industrial specifications and have been proving their long-lasting availability in identical formats for many years. CmDongles can store and manage the licenses and certificates of multiple providers simultaneously. Manufacturers of controller devices can use them to activate optional features; plant engineers can add their own license restrictions; and users can store their OPC UA certificates on the same dongle. The ability to store licenses of different origins is fully patented. It enables multiple users to use a single device to license their software and have all software packages running in parallel. This is a superior advantage of even the tiniest CmDongles.

Ready for Export

CodeMeter is available for export to all markets.

Licenses, Rights, and How to Manage Them

User rights and licenses can be allocated and managed at the function or device level. Any combination of licenses, features, and users is possible and individually configurable. Time and volume-based licenses, on-demand, pay-per-use or pay-per-click concepts are all possible.

License Reports for Users

The data produced by built-in analysis and monitoring tools with usage tracking are made available in reports to end users.

Licenses in the Cloud or Licenses on a Dongle

Wibu-Systems offers cloud, software, and dongle-based solutions. Cloud solutions are most effective when reliable Internet connections are available. However, manufacturing environments often operate without reliable Internet access, so dongle or local license files are more feasible options. Licenses for these offline solutions can be distributed via the cloud and then kept securely on a dongle or encrypted file. No machine will come to a standstill due to loss of Internet access. Saving licenses locally avoids unplanned stoppages.

Wibu-Systems Partners

Wibu-Systems cooperates with strategic partners in the embedded computing industry as well as the manufacturers of operating systems, controllers, and tools. OEMs can integrate CodeMeter's protection and licensing technology into their devices without any complex changes to the components in their tool chains. Wibu-Systems is the official protection and licensing partner of Wind River, and CodeMeter has been integrated effectively in many controller systems, such as Rockwell or B&R controllers.

Supported Microcontrollers

- Infineon XMC4000 series

Supported Operating Systems (selection)

- VxWorks
- QNX
- Windows
- Linux
- OS X
- Embedded Linux
- Windows Embedded Standard (WES)
- Windows Embedded Compact (WEC)

Controllers and Tools

- Bernecker and Rainer Industrie Elektronik Ges.m.b.H.
- CODESYS of 3S-Smart Software Solutions GmbH
  Hardware-independent IEC-61131-3 automation software for controller applications

Standards and Certificates

- OPC UA

Make or Buy?

This question is always the elephant in the room: use a popular industrial-grade and professional solution like CodeMeter or rely on one's own developers to implement similar protection? Security experts have a rule of thumb: "Standard solutions tested by experts offer greater security than bespoke solutions with secret codes or concepts."

But apart from the major security issue, the constant effort required to maintain and develop a custom solution should never be underestimated. The challenges and requirements change every day, cryptography is evolving, and new operating systems and components are invented. From a security standpoint, an outdated protection scheme is worse than no protection at all.

With CodeMeter, the OEM stays in control. He integrates CodeMeter in the software and hardware and can swap it out for a custom solution at any point. This means that OEMs can rely on a standard without being shackled to it forever.

A Successful Journey through the Internet of Things (IoT)

The Gartner study **"Competitive Landscape: License and Entitlement Management for 'Things' in the Internet of Things"** praises the following traits of Wibu-Systems' solutions:

- Focus on device-level security
- A versatile range of hardware-based protection that fulfill exacting industry standards
- Strong continuity with constant updates even for legacy products
- Licenses and rights managed via the cloud
- A large number of available licensing models
- Support for concurrent / floating, borrowed, and usage-based licenses
- Extremely small device runtime footprint (CodeMeter µEmbedded 60 kByte to 170 kByte)
- Support for all operating systems via source code
- OPC UA support
- Secure boot for embedded devices

Conclusions

With its many promises and great prospects, the IoT warrants much stronger protection than the closed systems of the past. Safeguards against reverse engineering and manipulation are required along the entire design chain – from the hardware to the individual application. Fine-grained licensing options are key for success. Wibu-Systems offers IoT-ready and scalable security products in robust, industry-grade versions. Equipped in this manner for the connected future, companies can look forward to lasting success in the new world of the Internet of Things.

Headquarters

WIBU-SYSTEMS AG
Rueppurrer Str. 52-54,
76137 Karlsruhe, Germany
Tel.: +49 721 93172-0
Fax :+49 721 93172-22
sales@wibu.com | www.wibu.com

WIBU-SYSTEMS Branch Offices

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 556 617 90
Beijing: +86 10 829 615 60
info@wibu.com.cn

WIBU-SYSTEMS NV/SA
Belgium | Luxemburg
+32 3 808 03 81
sales@wibu.be

WIBU-SYSTEMS sarl
France
+33 1 86 26 61 29
sales@wibu.fr

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.co.uk

WIBU-SYSTEMS BV
The Netherlands
+31 74 750 14 95
sales@wibu-systems.nl

WIBU-SYSTEMS IBERIA
Spain | Portugal
+ 34 91 123 07 62
sales@wibu.es

WIBU-SYSTEMS AG (WIBU®), a privately held company founded by engineers Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative technology leader in the global software licensing market.

In its mission to deliver unique, most secure and highly flexible technologies to software publishers and industrial manufacturers, Wibu-Systems has developed a comprehensive, award-winning suite of hardware- and software-based solutions incorporating internationally patented processes dedicated to the integrity protection of digital assets and intellectual property. Wibu-Systems' product portfolio addresses a wide variety of application delivery models, including PCs, mobile, embedded automation, cloud computing, SaaS, and virtualized architectures.

Through its motto "Perfection in Protection, Licensing and Security", Wibu-Systems is standing up for ethically produced software and reinforces its dedication to eradicate software counterfeiting, reverse-engineering, code tampering, as well as device and smart factory sabotage, espionage and cyber-attacks.

5062-007-02/20150911 ©2015 WIBU-SYSTEMS AG

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU
SYSTEMS