White Paper

CodeMeter in the Automation Industry

A Win-Win Opportunity for Producers of Machinery and Control Systems

Oliver Winzenried, CEO WIBU-SYSTEMS AG
www.wibu.com

WIBU SYSTEMS

Content

Author:
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 achieved at the University in Karlsruhe, he has immediately started an entrepreneurial career in electronic and ASIC design, hardware, microcontroller and embedded application development for consumer electronics, automotive and industrial engineering. Together with Marcellus Buchheit, in 1989 he then founded WIBU-SYSTEMS AG, whom he's still the CEO of. His passion for software integrity has resulted in numerous patent awards that span across secure license management and 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. His personal involvement in international R&D projects and organizations for standardization, such as the SD Card Association, tops his profile off. Oliver Winzenried is also serving as chairman in the Product Protection and Know-how Protection "Protect-Ing" committee of VDMA, in the board of directors of BITKOM as well as in the managing board of FZI at KIT.

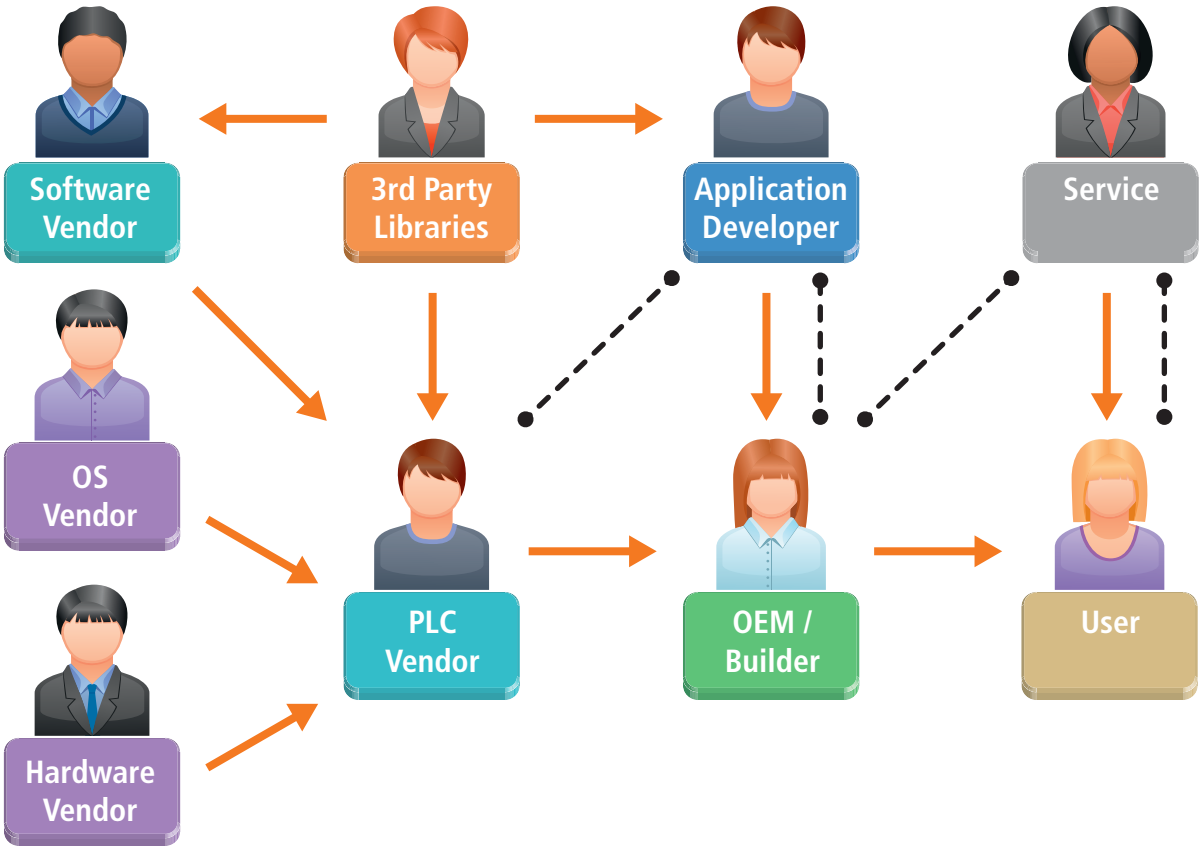
Introduction

Manufacturing equipment, from entire plants to individual machines, relies on the use of individual or multiple integrated control systems, typically including a combination of both hardware and software that plant engineers use to program the desired application. For the makers of control systems and manufacturing machinery, software can be an important USP (Unique Selling Point) as the indispensable key for many functions and applications. This whitepaper discusses the many competitive advantages that the makers and users of machines and their control systems can gain from CodeMeter. It also provides an overview of the concept and use of CodeMeter and the AxProtector encryption technology. Cost-conscious mechanical engineers must keep an eye on the price of effective control systems: Even in the high-investment field of mechanical engineering, an unchecked increase in the price of control systems cannot be accepted. Integrating protective technology like CodeMeter does come with upfront costs. Does the additional investment pay off? How much of the machinery costs are owed to its control systems? How will the control protections affect the long-term commercial prospects of the machine and how could a protection system influence the long-term prospects and performance of the engineering business? We will try to answer these questions for you in the following pages.

The Benefits of Protection

The integration of protection technology can prevent the copying of machine designs or the illicit transfer of essential know-how to competitors. The negligible additional investment can thus prevent millions of Euros' worth of potential damages and losses to the company. CodeMeter enables the producers of both control systems and manufacturing machines to launch new business models and expand their portfolios with minimal efforts. To name but a few examples: Effective license management solutions can control access and usage rights for certain functions or limit access to specific times. Features-on-demand license models can cater to individual demands of the customer while allowing the machine producer to keep his basic machine portfolio down to a manageable range of models. Protection against reverse engineering stops the illicit copying of their designs and helps protect both market share and brand image. Even the operators and users of the machines will benefit: Built-in integrity protection prevents sabotage and manipulation of the software. The system can also be used for scenarios in which production runs need to be limited to specific orders. The plant operator can offer to limit batch sizes in this manner as an additional service for the client, e.g. protecting against illicit 'third shift' production of luxury goods. The makers and users of production machinery and their controls thus benefit from the early and thorough integration of CodeMeter – a win-win outcome that control-system developers have the power to create. With a single product, they can get the upper hand on the threats described here and open up new business models at the same time. This is more than enough motivation for the developers of machine controls to integrate CodeMeter in their systems and a great argument for negotiating with the makers of manufacturing machines.

Automation involves different parties



Safe Foundations

Security begins at the start of the machine or plant engineering process. It concerns the following elements:

Controls and Development Environment

When plant engineers integrate control systems in their machines, the producers of the control system provide them with a development environment in the form of a dedicated software component. Each engineer on the project will have a personal development environment. It is in the interest of the producers of the control systems that these engineers will have the right licenses for their part of the development process. As the finished machine can include several controls, the package offered can thus include multiple development environments and control systems.

Hardware, RunTime Environments, and Operating Systems

A control system is basically a combination of hardware and a runtime environment, often using real-time operating systems like VxWorks, Windows Embedded, or Embedded Linux to operate, although there are runtime environments that can operate without an operating system around them.

The runtime environment is again a software component offered by the control system producer. It includes unique know-how and thus is an essential building block of the producer's business model that deserves to be protected.

IEC 61131 Programming Language and Applications

The maker of the machine uses the development environment provided by the control-system producer to script the desired application in an IEC 61131 programming language. The application tells the control system how the machine is to fulfill its intended purpose. The unique know-how of the machine engineer consists in this interaction between the machine and its controls. How sensors, motors, and axes work together determines how fast and precise the machine operates. Its capabilities are the USP of the machine engineer, and the end product of substantial investments into research and development. The assets invested in R&D for this purpose are intended to preserve the engineer's competitive advantage, an exceptionally valuable and sensitive asset.

Step-by-Step Protection with CodeMeter

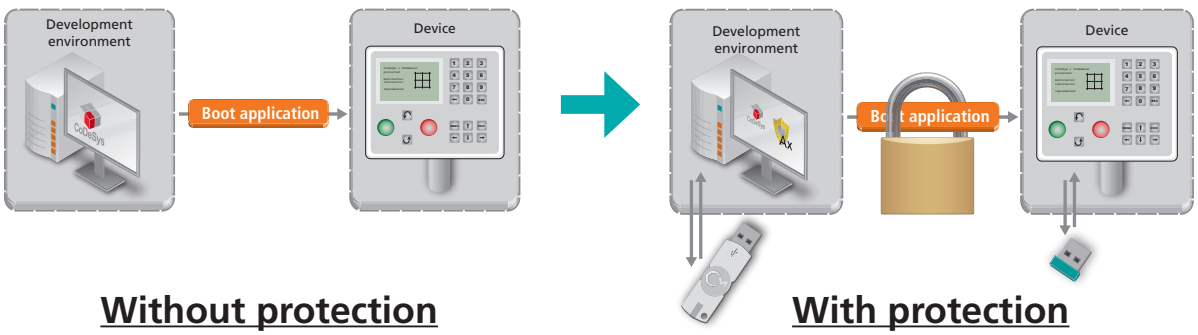
Operating systems, runtime environments, development environments, and applications form a secure chain.

Protected Applications in the Environment Development with the AxProtector Technology

First, the integrated development environment uses the AxProtector technology to encrypt the application before its transfer to the runtime environment. This step can be visualized with a container, in which the development environment locks the application, sealing it with a 'signature'.

Protected Applications in the Runtime Environment

The runtime environment in the control system recognizes that it has received the application in a closed container. It knows where to find the right key for that container and how to unlock it. Before it unlocks the container, it checks the signature (the seal). If the signature is valid, it opens the container and retrieves the application. This seal offers additional protection against sabotage. Unauthorized containers with malware are not opened. This protected route prevents hackers from tapping the transmission. The application thus moves from the development environment to the runtime environment in the most secure way possible.



The integrated protection via AxProtector ensures that the control runs only with dongle license and verified software

Protecting the Runtime Environment

Should an intelligent hacker try to interfere with the runtime environment, he would again come up against CodeMeter protections. Reliable protection needs the runtime environment to be booted securely. CodeMeter is available for many operating systems and runtime environments.

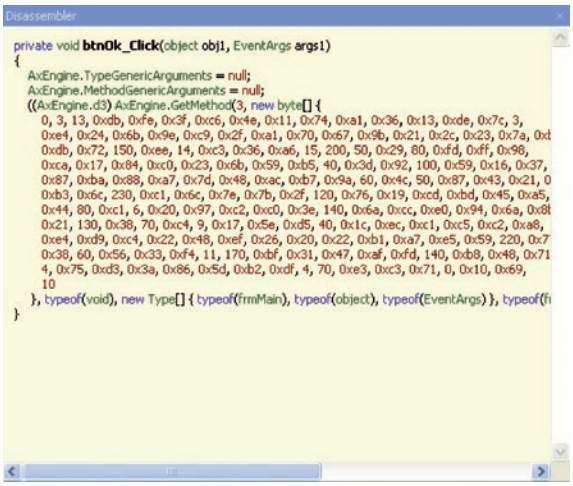
Foundations

The operating system, runtime environment, development environment, and actual application need to use CodeMeter and the AxProtector technology as a protection layer to enable all parties in this chain to benefit from the effective protection of their assets. The advantage of CodeMeter is evident: a single secure licensing solutions is enough to shield everybody. All licenses (even from multiple vendors) can be secured on a single dongle.

The Threats and Our Response:

Copycats by Reverse Engineering

CC, called Copy Cat, was the first cloned cat. Even though the clone had used the original genome, Copy Cat's fur differed from its clone mum. In global markets, the number of commercial copycats is on the rise. No sector of industry is immune: The producers of industrial equipment are suffering just as much as luxury goods or fashion brands. Counterfeiters benefit from saving the steep costs of R&D and using cheaper materials. They can operate at much lower costs. They undermine and upset established markets. Many copycats offer their products under the original brand, with their often poor quality damaging the image of the victim's brand. Flawless protection is impossible, but the rise of copycats can be checked. How do copycats operate? They read documents that are in the public domain. They scan product brochures, specifications, and manuals. They visit trade fairs and take pictures of their prey. They might simply buy the product to tear it down and measure its designs. None of this can be prevented. When it comes to reverse-engineering software, the copycats will encounter a formidable opponent in the form of CodeMeter and the AxProtector encryption technology. This is where reverse engineering fails – as long as CodeMeter and the AxProtector technology is used at all phases in the software's protection chain. As a closed chain, the protection covers the boot loader, operating system, runtime environment, the application, its parameters, settings, and even user's data. CodeMeter is available for many operating systems and runtime environments.



Functions, classes, and methods encrypted using AxProtector become unreadable for the hacker

Protecting against Reverse Engineering

Building a counterfeit copy of a machine is only possible if one has access to its operating software. Counterfeiters would try to extract the application code from the control system for reverse engineering: these attempts are blocked or made almost impossible with the AxProtector technology.

License Protection and Illegal Copies

Buy one, use many. This is the common fate of software.
Unethical people are known to supply their friends and acquaintances with software or engage in a thriving trade of other people's property. Copy a CD and write down the license number: Nothing is simpler to make than an illegal copy. It does not take long for many software packages to be installed from a single license. Simple license serial numbers and passwords are not effective protection. An integrated license protection system like CodeMeter creates much higher walls for criminals to climb. No hacker has yet broken the CodeMeter guard. The software developer's ROI is protected, because his product can only function if a valid license is present. He stays in control of his licenses by implementing and integrating CodeMeter. An implementation is only the first step as now the license process needs to be managed: license creation, license distribution, license updates, backup and restoration of licenses, and data mining with rich reporting. For all these tasks CodeMeter License Central is available as the single solution for creating and distributing licenses. It is integrated with the sales and distribution processes and streamlines the license publisher's business processes. Such license management and protection used to be limited to PC software, but software has long become an essential element of industrial machines and entire plants, where it is responsible for many functions. The risk of illegal copying must not be ignored in plant automation.

Export Controls

Control systems are universally applicable and have versatile designs. They are often subject to stringent export restrictions. The producers of such control systems are required to ensure that their products are not being sold to users in embargoed markets. To meet this requirement selective and restrictive sales to trusted engineering firms in combination with CodeMeter license protections is the answer. The license rights can be defined down to a level of individual functions. Selected critical features are license-protected and only operable with the right activation code. This level of protection means that the control-system developer fulfills his legal requirements in terms of export controls. The tamperproof recorded details of the licenses in CodeMeter License Central is evidence of the producer's due diligence. The same applies to the license holders. All licenses are stored in a dedicated container, either in a soft license file format or as industry-ready dongles.

Terrorism, Sabotage

Terrorism and sabotage are real threats in today's world. Cybercrime is on the rise. The terrorist and suicide bombers of old are joined by smart criminals who pursue their ends by manipulating technical systems. Their mission is to create substantial and high-profile damage, whether by traditional bomb or a blast caused by a control system that has been tampered with. Greed, revenge, and ideology have made people, machines, and products the target of increasing criminal attention. Control systems are ubiquitous: Driverless subway trains in cities, chemical plants, or wind farms in the countryside. Offsite maintenance and parameterization are open windows for cybercriminals wishing to access these controls. Most controls are located in closed networks, protected by VPN and firewalls. But do these means protect the controls themselves from illegal access? Access data for VPN can be stolen or gained by blackmail. Even good firewalls are not impenetrable for determined hackers. When a hacker has gained access to the network, most doors will be open to him. Behind the firewall, the control systems are laid bare. CodeMeter can protect against such illicit access to control systems. Every control system is a separate protected entity. CodeMeter-protected controls raise formidable barriers to hacking: the hacker is prevented from loading malware into the system or manipulate it for his criminal purposes.

Demo Devices

A clever terrorist would try to get access to the developer tools and prototype designs, but CodeMeter would be there to stop him. He could not manipulate the live system by reverse engineering the demo device, as separate key chains would prevent this. Fully functioning prototypes are thus incompatible with the final market system.

OPC UA with Security

OPC UA is an ISO standardized protocol for connected devices accessing the Internet, with offsite maintenance as a typical use case. The OPC-UA standard includes security specifications, but most instances use OPC UA without the security protocols. In everyday business, the greatest obstacle in this respect lies in the administration and allocation of keys and rights. Wibu-Systems solves this problem of access key management with CodeMeter License Central, which can also manage certificates. CodeMeter can be configured to integrate with OPC UA, using the protocols of OPC UA in full conformity with the standards. This enables OPC UA with security for authentication and encrypted communication.

Integrity Protection

Reliably protecting the integrity of a plant is an important sales argument. This also goes for guaranteeing the conformity of components: Industry-specific norms regulate the precise specifications of production equipment. Be they rail-certified, blast-proof, food-safe, vibration-resistant, or watertight, components are made and equipped for their intended purpose. The operators of production plants want assurances that all of their components and software are fully certified. CodeMeter allows this level of integrity protection with signed program code and inclusion in a trusted certification chain.

Manipulation

Every technical device is made for a specific area of operation, and its producer would guarantee its effective work under these terms and specifications. What are the implications for producers when their clients tamper with the equipment to modify it beyond its specified range? A modified motorcycle will be faster and louder – and soon be taken off the roads by traffic police. Their drivers will lose their insurance and be liable for hefty fines. A modified production plant might also be running faster and create additional profits, but their components would also wear down in record time. If the producer of the machinery cannot prove that the machines were running outside of the original specifications, he would have to provide the regular maintenance and warranty coverage. CodeMeter enables the makers of plant machinery to protect against the illicit changing of parameters or record any changes in a tamperproof log.

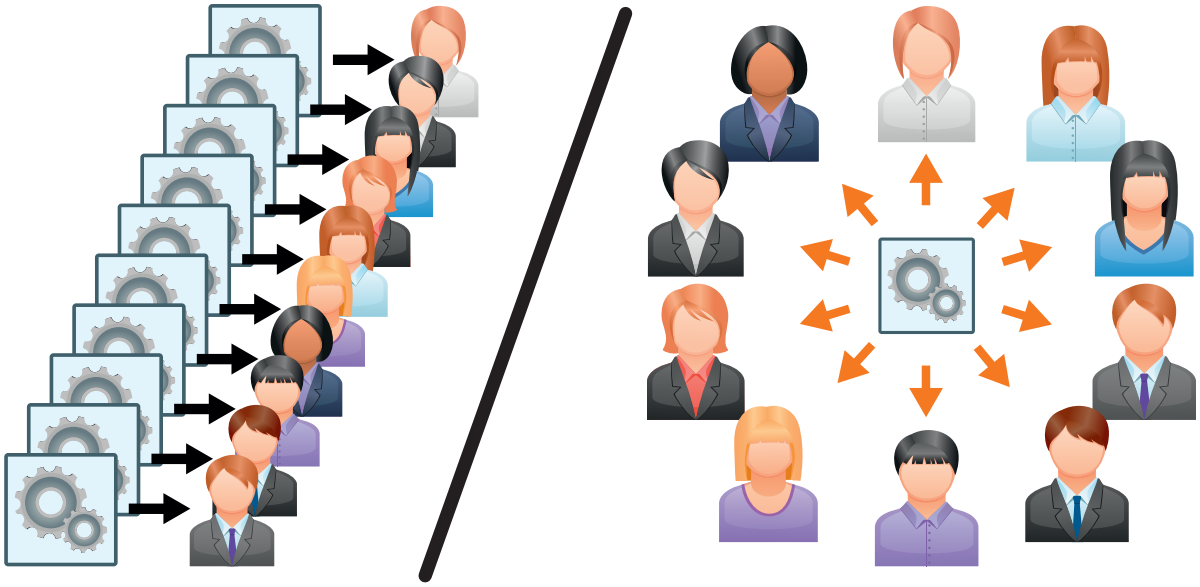
Modular Protection for the Plant Engineer's Source Code

Plant engineers usually possess the readable source code for their applications. Effective protections are now essential: By having access to the source code, the client could interfere with the internal workings of the machine. Having this opportunity to edit the source code can indeed be a reasonable requirement for qualified maintenance personnel, e.g. for taking less relevant defective sensors offline to keep production processes running until the sensor is repaired at the next maintenance interval. By contrast, parts that are critical for security and for protecting the plant engineers' essential know-how must be shielded from such external access. The client should not be able to copy and pass on functioning source code to unauthorized third parties. Again, the licensing mechanisms offered by CodeMeter are an effective barrier. Not only the clients of plant engineers, but also their employees have access to the source code. Developers write the machine applications in an IEC 61131 language, for which they need access to readable source code. Maintenance technicians need to work with the source code in their routines. By force or enticement, a criminal counterfeiter could use these staff members as an open door to the code. Source code needs to be protected against unfaithful employees and disloyal clients alike. CodeMeter guarantees that protection: The counterfeiter might get the source code, but he could never produce an executable application for it.

New Business Models

Reducing Production Costs

The costs of production can be brought down when multiple variants are covered with a single product, which also makes for easier and more cost efficient product management. Software products are a perfect candidate for this model, as long as their developers can protect the available variants against illicit use. A machine control system might be able to control multiple axes, but the maker of a machine that only needs to control two axes would only expect to pay for these two axes. For the machine developer, it is of no relevance whether the software can control an additional six axes. In this scenario, the developer of the control system would provide software with the functionality to manage eight axes, but the license acquired by the client only activates the controls for two axes. The license is managed and processed with CodeMeter License Central. The many licensing options made available by CodeMeter give the maker of the control system the opportunity to design a rich selection of usage rights as part of the product. At the same time, the developer only has to manage one master product, with the personalized licenses provided at the time of need: A lean production process whose simplicity is mirrored by the granular licensing options made possible by CodeMeter License Central.



Leaner logistics: Instead of 10 individual machines for 10 customers only a single one-in-all machine exists configured via licenses.

Features on Demand

When developing production plants, mechanical engineers might come to realize that they need further controls to operate additional axes. They would buy additional licenses for activation in their existing software to control these axes. This requires no new software to be installed: The producer of the control system can quickly respond to this new requirement and provide an individually scalable solution for a basic standard product. This allows plant engineers to sell and activate additional features for their clients, creating new business opportunities on both sides.

Temporary Licenses

Sometimes, users simply want to test software to get to know its capabilities or run benchmark tests. Ideally, they want access to a full version of the software, but the software developer has to make sure that these demo versions are not utilized for illegal permanent use. Temporary licenses are the answer. Time, volume, or function-limits can be freely combined.

Keeping Tabs on Service Technicians

Time or volume-limited licenses are also relevant for installation, maintenance, and repair services. Technicians often require extensive access rights to be able to do their work. Security demands that these rights are limited only to the period of their active work at the client site. The license expires immediately after the service has been provided and is thus useless for anybody vying for unauthorized access.

Volume-Limited Licenses

The system allows the number of accesses to a function or software application to be limited. This limitation option creates interesting new business opportunities for mechanical engineers, as it allows product designs to be restricted to a defined production run or batch size. The machine itself becomes a first line of defense against illicit products like expensive designer fashions being produced in clandestine 'third shifts' and placed into the black market trade.

Retrofitting Control Systems

Not every control system is equipped with CodeMeter functionality, but retrofitting existing machinery poses no technical problems. Wibu-Systems' dongles are industry-ready and available for many different interfaces. This includes CmSticks as USB dongles or CmCards in SD Card, microSD Card, or CompactFlash Card format. The robust sticks and cards function reliably in a broad range of temperatures and are protected against condensation by conformal coating. Licenses for CmDongles or CmActLicense files containing activations for the target control system can be transferred both online and offline, making the system an appealing option for machinery lacking network access.

Summary

It is up to the producers of industrial control systems to achieve a win-win situation for their partners by using CodeMeter and the AxProtector technology. All they need is readily accessible at their fingertips, as CodeMeter protection is already available for many operating systems and has been implemented in development systems like CODESYS or Bernecker & Rainer's Automation Studio.

A decision in favor of CodeMeter offers the producers of control systems and their partners many benefits:

- Protection against reverse engineering
- Protection against illegal copying
- New business opportunities with features-on-demand
- Improved export controls
- Integrity and manipulation protection
- Tamperproof logs
- Protection against sabotage
- Control over demonstration units
- Simplified logistics with software licensing for machines
- Reduced production costs
- Protection for R&D investments and technological advantages

The protections can be retrofitted in existing control systems by simple software updates. CodeMeter offers a single standard means for managing access rights, certificates, keys, and licenses in a fully scalable solution for all use cases described here. The CodeMeter licenses are stored in a dedicated license container, either a dongle or license file. The container can store licenses for multiple rights holders, like the makers of the control systems or production machines or the commissioning client. Wibu-Systems' CodeMeter dongles are designed to be industry-ready.

Headquarters

WIBU-SYSTEMS AG
Rueppurrer Str. 52-54,
76137 Karlsruhe, Germany
Telephone: +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 USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

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

WIBU-SYSTEMS NV/SA
Belgium | Luxembourg
+32 3 400 03 14
sales@wibu.be

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

WIBU-SYSTEMS IBERIA
Spain | Portugal
+ 34 91 414 8768
sales@wibu.es

WIBU-SYSTEMS sarl
France
+33 1 73 03 04 91
sales@wibu.fr

5062-003-01/20140508

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.

Headquartered in Karlsruhe, Germany, Wibu-Systems holds subsidiaries in Seattle, USA, as well as in Shanghai and Beijing, China; the company also has sales offices in Belgium, France, the Netherlands, Portugal, Spain, the United Kingdom and a capillary world distribution network.

© 2014 Wibu-Systems. WIBU®, CodeMeter®, SmartShelter® are registered trademarks of Wibu-Systems. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU SYSTEMS