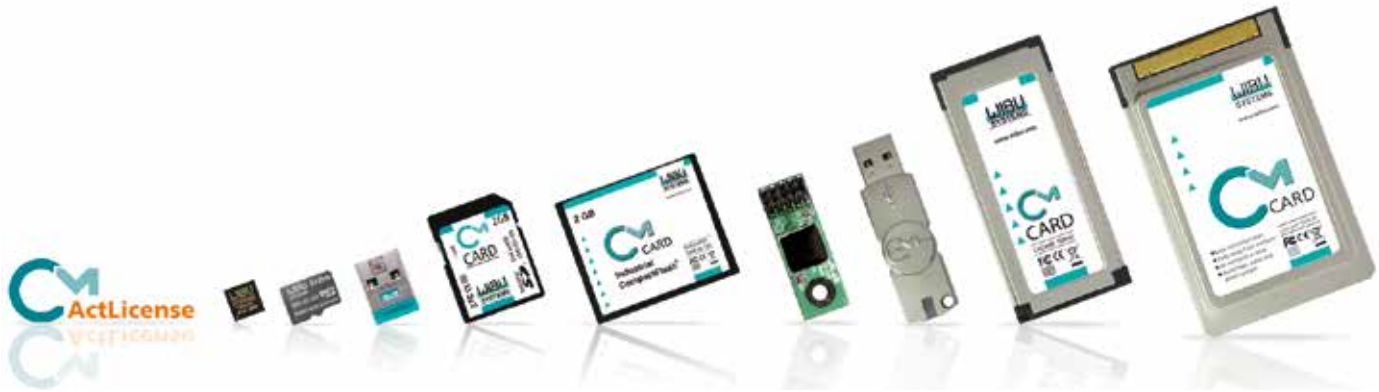
Produkte und Know-how in der Industrie schützen

Produktpiraterie verursacht jährlich Schäden in Milliardenhöhe – Tendenz weiter steigend. Deshalb gilt es, Hard- und Software besser zu schützen. Wibu-Systems stellt eine Technologie in zwei Varianten bereit, sodass sie sowohl software- als auch hardwarebasierten Schutz bietet.

Oliver Winzenried



Die Schutzhardware „CmDongle“ von Wibu-Systems ist in verschiedenen Bauformen verfügbar

Die Zeiten, in denen die Funktionen einer Maschine allein von ihrem mechanischen Aufbau oder einer einfachen Steuerelektronik festgelegt wurden, sind vorbei. Heutzutage bestimmt zu einem großen Teil die Embedded-Software der Maschine, was sie kann. Das eröffnet dem Hersteller neue Möglichkeiten. So kann er zum Beispiel Maschinen ausliefern, bei denen nur die Funktionen freigeschaltet sind, für die der Kunde bezahlt hat (Feature-on-Demand). Leider entstehen mit den neuen Möglichkeiten auch neue Gefahren: Je mehr die Funktion einer Maschine von ihrer Embedded-Software abhängt, desto mehr Know-how steckt in der Software – wertvolles Wissen, für das sich Produktpiraten interessieren. So haben auch sie mittlerweile erkannt, dass es nicht mehr genügt, nur die mechanischen Teile einer Maschine oder Anlage nachzubauen. Zudem wächst die Gefahr von Sabotage, da Software leichter zu manipulieren ist als Hardware. Um diese Gefahren abzuwehren, müssen die Hersteller geeignete Vorkehrungen treffen.

Oliver Winzenried ist Vorstand der Wibu-Systems AG.

E-Mail: info@wibu.com

Schäden in Milliardenhöhe

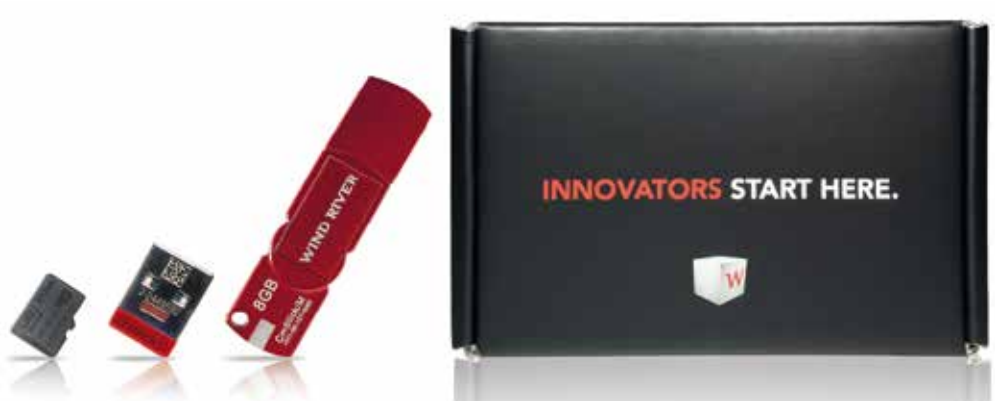
Die Schäden durch Produktpiraterie gehen mittlerweile in die Milliarden. Um sie genau zu beziffern, befragen unter anderem Verbände ihre Mitglieder. So beispielsweise auch der Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA). Im April 2012 führte er eine Mitgliederbefragung zum genannten Thema mit folgendem Ergebnis durch: Zwei Drittel der Unternehmen sind von Produkt- und Markenpiraterie betroffen. Hauptsächlich werden Komponenten plagiiert, gefolgt vom Nachbau ganzer Maschinen. Der geschätzte Schaden beträgt rund 8 Mrd. € und ist damit um ein Viertel gestiegen, verglichen mit der letzten Studie aus dem Jahr 2010.

Auch in Japan fand im Oktober 2012 eine Befragung statt. Der japanische Maschinenbauverband JMF hat seinen Mitgliedern die gleichen Fragen gestellt wie der VDMA. Ergebnis: Fast die Hälfte der befragten Unternehmen ist von Produktpiraterie betroffen; der Schaden beträgt umgerechnet 13 Mrd. €.

Einen Grund für die höhere Schadenssumme sieht der VDMA darin, dass japanische Unternehmen bisher kaum technische Abwehrmaßnahmen ergreifen.

Geeignete Maßnahmen zum Produkt- und Know-how-Schutz

Seit mehr als zwanzig Jahren unterstützt die Karlsruher Wibu-Systems AG Unternehmen beim Schutz ihrer Produkte und ihres Know-hows durch präventive Lösungen. Diese Lösungen basieren auf der sicheren Verschlüsselung von Software jeglicher Art, also auch der Embedded-Software im Maschinen- und Anlagenbau. Damit verhindern sie die Analyse (Reverse-Engineering) und den Nachbau von Maschinen und Anlagen durch Produktpiraten. Mit hohem Schutzniveau, Flexibilität, Praxistauglichkeit, einfacher Nachrüstbarkeit in bestehende Systeme



Das neue Embedded Development Kit von Wibu-Systems, Emerson Network Power und Wind River enthält drei Code-Meter-Komponenten

und der Einhaltung industrieller Standards erfüllt die Code-Meter-Technologie von Wibu-Systems die Anforderungen der Industrie. Code-Meter ist vielfältig einsetzbar, egal ob es um klassischen Softwareschutz geht, Integritätsschutz oder die Abbildung flexibler Geschäftsmodelle wie Pay-per-Use oder Feature-on-Demand.

Die Technologie wird in zwei Varianten angeboten: dem softwarebasierten Schutz „CmActLicence“ und dem hardwarebasierten Schutz „CmDongle“. Erstgenannte basiert auf sicheren Aktivierungsdateien. Die Schutzhardware enthält eine Smart-Card-basierte Sicherheitskomponente und ist für viele Schnittstellen, zum Beispiel USB, SD, Micro-SD oder Compact-Flash, erhältlich. Beide Varianten funktionieren auf Standardbetriebssystemen, wie Windows 32/64-bit, Mac OS oder Linux, oder auf speziellen Systemen und Steuerungen der Industrie, wie dem Echtzeitbetriebssystem „VxWorks“ oder der IEC-61131-3-Entwicklungsumgebung Codesys.

Code-Meter nutzt moderne und sichere Verschlüsselungsverfahren, wie die symmetrische Verschlüsselung AES (Advanced Encryption Standard) mit 128-bit-Schlüsseln und die asymmetrische Verschlüsselung ECC (Elliptic Curve Cryptography) mit 224-bit-Schlüsseln.

Flexible Geschäftsmodelle für die Industrie

Hersteller können in der Embedded-Software festlegen, welche Funktionen ihrer Maschinen, Anlagen oder Geräte ein Kunde nutzen kann. Beim Kauf erhält der Kunde das Produkt zusammen mit der kompletten, verschlüsselten Embedded-Software. In der „CmActLicense“-Datei oder dem „CmDongle“ werden jedoch nur die gekauften Funktionen freigeschalten, das heißt die Nutzungsrechte werden sicher in der Schutzhardware oder der Aktivierungsdatei gespeichert. Dies vereinfacht die Logistik, denn jeder Kunde bekommt das gleiche Produkt, das alle Funktionen enthält, von denen er aber nur die vereinbarten nutzt.

Zusätzlich kann der Hersteller flexible Geschäftsmodelle, wie Feature-on-Demand, Pay-per-Use oder Demo-Versionen, für seine Kunden abbilden. Der Kunde bekommt genau das, was er möchte, und kann nachträglich weitere Funktionen oder Nutzungseinheiten nachkaufen oder die Demo-Version zur Vollversion umwandeln lassen.

Zur Verwaltung der Nutzungsrechte steht den Mitarbeitern des Herstellers die Software Code-Meter License Central zur Verfügung. Damit können sie auf einfache Weise Nutzungsrechte erzeugen, verwalten und für eine bestimmte „CmActLicense“-Datei oder einen bestimmten „CmDongle“ bereitstellen. Darüber hinaus lässt sich die Code-Meter License Central in Vertriebsprozesse und vorhandene ERP- oder Shopsysteme integrieren.

Produkt- und Know-how-Schutz in der Praxis

Code-Meter kann für verschiedene Zwecke in der Industrie eingesetzt werden und neue Anwendungsfälle kommen ständig hinzu:

- Schutz von Embedded-Software für „VxWorks“: Als Ergebnis der Zusammenarbeit von Wind River, dem Anbieter des Echtzeitbetriebssystems „VxWorks“, und Wibu-Systems wurde Code-Meter in „VxWorks“ integriert, beginnend ab der Version 6.8. Somit können Entwickler ihren mit „VxWorks“ erzeugten Code vor Produktpiraterie schützen. Zu den Einsatzmöglichkeiten zählen: Schutz des Programmcodes vor Manipulation, das sichere Booten des Betriebssystems oder das sichere Betreiben einer Anwendung.
- Nutzungsrechte im „CmDongle“ oder in der „CmActLicense“ sicher speichern: Der Steuerungsanbieter Rockwell Automation setzt Code-Meter zur Zugriffskontrolle für den Quellcode ein. Nur wenn der Entwickler das richtige Passwort mit der entsprechenden Berechtigungsstufe hat, kann die Entwicklungssoftware Studio 5000 Logix Designer genutzt werden. Die traditionelle Authentifizierung über Benutzername und Passwort wird durch die Code-Meter-Technologie ersetzt, um die Nutzungsrechte sicher zu speichern. Somit kann der Quellcode nicht von Unbefugten verändert werden und ein absichtliches oder unbemerktes Weitergeben von Benutzername und Passwort ist unmöglich.
- Schutz von Automatisierungssoftware: Automatisierungshersteller, die mit der Version 3.5 oder höher der IEC-61131-3-Entwicklungsumgebung Codesys von 3S-Smart Software Solutions GmbH arbeiten, können ihren Code mithilfe von Code-Meter verschlüsseln, bevor dieser auf das Zielsystem übertragen wird. Die Nutzungsrechte liegen in der „CmActLicence“-Datei oder im „CmDongle“. Ist die richtige Lizenz vorhanden, wird die Software entschlüsselt und ausgeführt.

Ausblick

Moderne Schutzsysteme wie Code-Meter erfüllen die heutigen Anforderungen der Hersteller an Produkt- und Know-how-Schutz. Damit ein Entwickler schnell und effektiv mit einem Schutzsystem arbeitet, benötigt er geeignete Werkzeuge, die jede seiner Anforderungen erfüllen. Dies können sichere Verschlüsselung oder Freischaltung von Funktionen der Maschine, Anlage oder des Geräts sein. Auf diese Weise kann sich der Entwickler auf seine eigentliche Arbeit konzentrieren und sich beim Schutz auf das zugekaufte Schutzkonzept verlassen.

www.wibu.com