Die Gefahren der Digitalisierung

LIVE@ HANNOVER MESSE

Präventiver Schutz für Anwendungen der Automatisierungsindustrie

01 Die CodeMeter-Technologie kann einfach nachgerüstet werden und ist in unterschiedlichen, industrietauglichen Bauformen verfügbar

Immer mehr Funktionen stecken in Software und Daten. Sie legen fest, wie eine Maschine, Anlage oder ein Gerät arbeitet. Geschlossene Infrastrukturen weichen vernetzten Systemen. Zudem werden nicht mehr nur Maschinen, Anlagen oder Geräte verkauft, sondern auch nur einzelne Funktionen. Lesen Sie, welche Gefahren sich hinsichtlich Daten- und Manipulationssicherheit dadurch ergeben und wie Sie Ihr Know-how schützen können.

Damit nun die Digitalisierung von Produkten und Prozessen funktionieren kann, sind geeignete Schutzmechanismen erforderlich. Seit über 15 Jahren entwickelt Wibu-Systems die Schutztechnologie CodeMeter als technisch präventiver Schutz weiter, um die unterschiedlichen Bedürfnisse der Automatisierungsindustrie zu erfüllen. Mögliche Maßnahmen sind:

- Mithilfe von Verschlüsselung werden Geräte-know-how sowie Daten geschützt
- Schutz vor Produktpiraterie durch nichtkopierbare Schlüssel, dass heiß der sicheren Hardware CmDongle
- Die Geschäftsprozessintegration mit dem Tool CodeMeter License Central erlaubt, ganz flexibel Funktionen freizuschalten.
- Digitale Signaturen
- Ein hoher Level an Sicherheit entsteht, denn die digitale Identität für alle vernetzten Systeme, Schutz der Kommunikation sowie Integritätsschutz für Daten und Software ist gewahrt
- Viele Hersteller können sich eine Schutzhardware teilen, wobei jedoch jeder seine Einträge ändern kann.
- Standardisierte Kommunikationsprotokolle wie OPC UA erlauben Kommunikationssicherheit für Cyber Security
- Sowohl die CmDongles als auch die softwarebasierten Aktivierungsdateien können einfach nachgerüstet werden, sodass auch langlebige Maschinenparks mit Know-how- Schutz ausgestattet werden können.

Oliver Winzenried *ist Vorstand der Wibu-Systems AG und der AG Medizintechnik im VDMA in Karlsruhe*

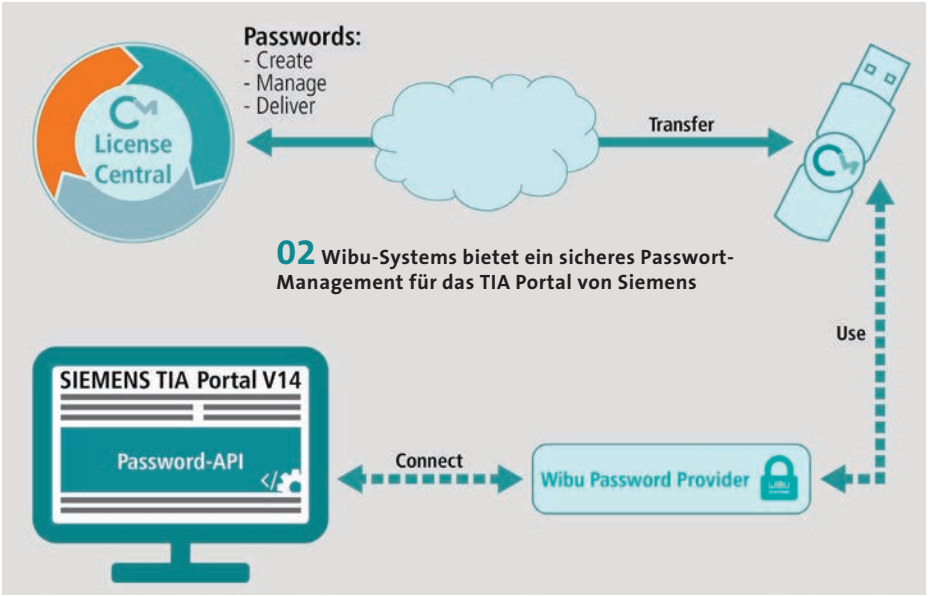
Wie funktioniert die Schutztechnologie CodeMeter?

Das Herzstück von CodeMeter ist die Speicherung kryptografischer Schlüssel gemeinsam mit Lizenzbedingungen und Optionen wie Pay-Per-Use-Zähler, Zeitbegrenzung, Named-User oder Floating Licenses und so weiter. Dies erfolgt in CmDongles oder rein softwarebasiert in Aktivierungsdateien durch Bindung an einen Fingerabdruck des Zielsystems. Darüber hinaus bietet CodeMeter dem Softwarehersteller Tools und ein API zum Ver- und Entschlüsseln sowie zum Signieren. Für die Integration in die Geschäftsprozesse und ERP- oder E-Commerce-Anwendungen dient die CodeMeter License Central, die wahlweise in der Cloud betrieben wird.

Für einen hohen Sicherheitsgrad bei CodeMeter sorgen moderne und sichere Verschlüsselungsverfahren wie die symmetrische Verschlüsselung AES (Advanced Encryption Standard) und die asymmetrische Verschlüsselung ECC (Elliptic Curve Cryptography) oder RSA.

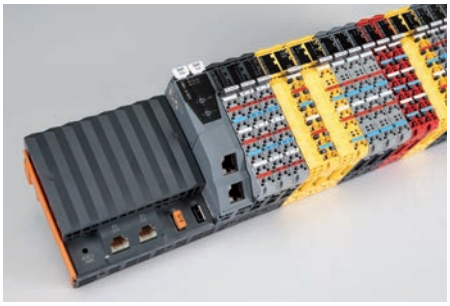
Sicheres Passwort-Management für das TIA Portal von Siemens

Mit dem TIA Portal können Maschinen- und Anlagenbauer auf ein Software-Komplettpaket zugreifen, das Funktionen zur Automatisierung und Digitalisierung effizient und beherrschbar verknüpft. Im Portal werden Engineering-Daten gespeichert, die oft schützenswertes, wertvolles Know-how enthalten. Ab der Version 14 SP 1 des TIA



02 Wibu-Systems bietet ein sicheres Passwort-Management für das TIA Portal von Siemens

Portals können die Benutzer den von Wibu-Systems entwickelten Passwort-Provider, der mit der Passwort-API von Siemens verknüpft ist, nutzen. Anstatt die Passwörter nur geheim zu halten, werden die Passwörter sicher in CmDongles gespeichert. Die Zugangskontrolle über Nutzungszeitraum, Ablaufdatum oder einen Nutzungszähler legt fest, wie die Benutzer auf Engineering-Daten zugreifen oder ob sie diese verändern können. So wird sichergestellt, dass nur berechtigte Benutzer die Projekte sehen und bearbeiten können, für die sie volle Rechte haben.



03 **Klein und unauffällig steckt der orange-farbene CmStick/C Basic auf dem Automatisierung-PC von B & R**

Konkrete Projekte zeigen die Integration in Steuerungen

Damit Hersteller im Maschinen- und Anlagenbau ihren Programmcode schützen können, haben verschiedene Steuerungsanbieter die CodeMeter-Technologie bereits in die Engineering-Werkzeuge ihrer Steuerung integriert. Analog zu der Funktion „Drucken“ im Word können die Anwender mit einer Funktion „Schützen“ in der Steuerung arbeiten, um wiederum das Ergebnis ihrer Arbeit zu schützen. Zu den Lösungen der Steuerungsanbietern zählen u. a. B&R Automation Studio, Codesys, Rockwell Software Studio 5000 Logix Designer und Siemens TIA-Portal.

B&R hat CodeMeter in die Entwicklungstools von Automation Studio und in die Runtime ihrer Automatisierungs-PCs integriert; jeder Automatisierungs-PC wird mit einem CmDongle ausgeliefert, der das Know-how und die dazugehörigen Lizenzen schützt. 3S-Smart Software Solutions schützt mit CodeMeter den Quellcode von Projekten und des Zielsystems im Codesys-Entwicklungstool und in der Codesys Runtime. Die Lizenz zur Nutzung wird im CmDongle gespeichert.

Zusammen mit Rockwell Automation hat Wibu-Systems den lizenzbasierten Schutz „License-based Protection“ entwickelt. Das ist eine Security-Suite, die aus drei Komponenten besteht: dem Schutz des sensiblen Quellcodes, Schutz bei der Ausführung in Controllern und es enthält ein Web-Portal zur Verwaltung von Lizenzen und Berechtigungen. Die Berechtigungen werden als Lizenzen sicher in CmDongles gespeichert.

Sicherheit und Lizenzen im Transportwesen

ABB als globaler Player ist auch im Bereich industrielle Automation aktiv. Im Transportwesen ist die Software ABB Ability Schifffahrtinformationssystem Octopus von ABB Marine & Ports mit dem CmStick ME im robusten, seetauglichen Metallgehäuse geschützt. In der nächsten Version der Octopus-Suite wird zusätzlich zum CmStick ME auch die softwarebasierte Lösung CmAct-License eingesetzt und das Ausleihen und die Aktualisierung der Lizenzen erfolgt über die Cloud. Die Aktivierungsdateien werden an den digitalen Fingerabdruck des Geräts oder Computers auf dem Schiff gebunden, auf dem die berechtigte Lizenz läuft.

Know-how-Schutz in einem Engineering-Tool

PC Worx Engineer ist eine Engineering-Plattform passend für das neue Automatisierungssystem mit PLCnext Technology von Phoenix Contact. Die Grundversion der neuen Engineering-Plattform ist kostenfrei. Angepasst an ihre Applikation können Anwender jederzeit weitere Funktionen als Add-ins erwerben. Um das Know-how in diesem Engineering-Tool zu schützen und die Nutzung abzurechnen, setzt Phoenix Contact die CodeMeter-Technologie von Wibu-Systems ein und verschlüsselt die komplette Software mit dem Tool AxProtector. In den softwarebasierten Aktivierungsdateien von CmActLicense werden die Nutzungsrechte gespeichert und an die PC-Hardware gebunden, auf der PC Worx Engineer installiert ist.

Im Hintergrund des Online-Shops von Phoenix Contact erzeugt, verwaltet und verteilt die CodeMeter License Central automatisch alle Tickets, die anschließend über einen Internet-Zugriff oder Offline-Prozess aktiviert werden können. Zusammen mit dem Installationspaket von PC Worx Engineer erhält der Anwender eine kostenfreie Demo-Lizenz mit einer Laufzeit von 30 Tagen. Permanente Arbeitsplatzlizenzen oder kostenpflichtige Netzwerklizenzen können jederzeit mit dem gewünschten Funktionsumfang über den Online-Shop von Phoenix Contact konfiguriert und bestellt werden. Der Anwender erhält dann ein Ticket mit der Nutzungslizenz per E-Mail und kann hierüber die Nutzungsrechte organisieren.

Bilder: *Wibu-Systems*

www.wibu.com