Intelligenter Schutz des geistigen Eigentums

Die »CmDongles« in verschiedenen Bauformen sind für den harten Fabrikalltag geeignet, denn gute elektromagnetische Verträglichkeit oder Hitzebeständigkeit wurden bei der Entwicklung berücksichtigt. Bild: Wibu

Intelligente Produktion zeichnet sich durch vernetzte Maschinen und Anlagen sowie durch Prozesse aus, die zur Auftragslage passen, flexibel und effizient sind. Einerseits bringt diese Veränderung in Richtung Industrie 4.0 Herstellern in der Automatisierungsindustrie interessante Möglichkeiten für neue, intelligente Produkte. Andererseits steigt die Gefahr, dass Wirtschaftsspione, Produktpiraten und Saboteure an das Knowhow in der Software herankommen, in sensible Produktionsnetzwerke eindringen und die Produktion stören oder Maschinen und Anlagen beschädigen.

Autoren:
Elke Spiegelhalter
Presse- und Öffentlichkeitsarbeit
WIBU-SYSTEMS AG
76137 Karlsruhe
www.wibu.com

Roland Wagner
Head of Product Marketing
3S-Smart Software Solutions GmbH
87439 Kempten
www.codesys.com

Bereits seit 2012 kooperieren 3S-Smart Software Solutions GmbH, Hersteller der hardwareunabhängigen IEC 61131-3-Automatisierungssoftware »Codesys«, und Wibu-Systems AG, Hersteller der »CodeMeter«-Technologie zu Schutz, Lizenzierung und Security. Beide Unternehmen haben die unterschiedlichen Schutzbedürfnisse der Anwender aus dem Bereich Automatisierung analysiert und das passende Schutzkonzept entwickelt. Als Resultat enthalten alle Entwicklungsumgebungen ab Version 3.5 der Automatisierungssoftware die Schutzlösung. Die Anwender können damit ihr Knowhow vor Reverse Engineering und unberechtigtem Nachbau schützen sowie Zusatzfunktionen bequem im »Codesys«-Store erwerben und lizenzieren.

Schutz des SPS-Quellcodes

Anwender erstellen den Quellcode der Steuerungsapplikation in den Sprachen der IEC 61131-3 mit dem Entwicklungssystem auf ihrem Arbeitsplatzrechner. Damit sind die Maschinenfunktionalität sowie das persönliche Knowhow des Applikationsentwicklers in der Software codiert – ein schutzwürdiges Gut! Die Verschlüsselung des Quellcodes ist zwar per Passwort möglich, aber durch eine unkontrollierte Weitergabe des Passworts schnell wieder unwirksam. Zudem wäre der gesamte Quellcode verloren, wenn das Passwort nicht mehr zur Verfügung stünde. Der Knowhow-Schutz per Dongle mag zunächst weniger komfortabel erscheinen, hat aber entscheidende Vorteile: Mit dem vorprogrammierten Security Key, einem USB-Dongle mit »CodeMeter«-Technologie, kann der Anwender den Quellcode zum einen per Hardware so verschlüsseln, dass er auch mit viel Aufwand nicht mehr gehackt werden kann, zum anderen kann er ganz genau kontrollieren, an wen er den Schlüssel und damit den Zugang zu seinem Projekt gibt. Dabei ist es möglich und ratsam, mindestens einen zusätzlichen Schlüssel für den Zugriff auf das Projekt zu registrieren, der dann zum Beispiel im Tresor des Unternehmens hinterlegt wird.

Gleichgültig, ob das Projekt nun per E-Mail oder Datenträger weitergegeben oder sogar im Quellcode auf der Steuerung abgelegt wurde: Es kann nur geöffnet werden, wenn einer der hinterlegten Keys am Arbeitsplatz angeschlossen ist. Im Dongle selbst sind ein eindeutiger, individueller Firm Code und ein Product Code gespeichert, sodass es nicht ausreicht, irgendeinen Security Key oder Dongle gleicher Bauart gesteckt zu haben.

Schutz der Steuerung

Nachdem der Applikationsentwickler den Code erzeugt hat, wird dieser vom Entwicklungssystem in ausführbaren Binärcode kompiliert und auf das Zielgerät übertragen. Ist die Applikationsentwicklung beendet, so wird der hinterlegte Code per Kommando zur Bootapplikation, die beim Einschalten des Geräts automatisch startet. Nachdem die meisten modernen Steuerungen heute über ein mehr oder weniger zugängliches Betriebs- und Dateisystem verfügen, könnten Raubkopierer auf die Idee kommen, statt des Quellcodes die kompilierte Applikationssoftware unberechtigt zu vervielfältigen, zum Beispiel, indem die Maschine nachgebaut, mit der gleichen Steuerung ausgestattet und dann der kopierte Binärcode darauf übertragen wird. Dreiste Kopierer könnten versuchen, durch Disassemblieren oder Dekompilieren an den Quellcode zu kommen oder sogar die Steuerung nachzubauen und die kopierte Firmware darauf abzulegen. Die im »Codesys«-Control-Laufzeitsystem integrierte »CodeMeter«-Technologie kann solche Szenarien verhindern. Für einen absolut sicheren Schutz kommen wiederum zusätzliche Hardware-Komponenten zum Einsatz, die »CmDongles«. Im Innern eines jeden Dongles befindet sich ein SmartCard-Chip, der die Ver- und Entschlüsselung übernimmt, und zwar mit anerkannten Algorithmen wie AES, ECC und RSA. Die Dongles sind in ganz unterschiedlichen Bauformen wie USB, SD, microSD, CFast oder CompactFlash verfügbar und können auf nahezu jedem Automatisierungsgerät integriert werden. Sie sind für den Einsatz im harten Fabrikalltag ausgelegt, denn Kriterien wie gute elektromagnetische Verträglichkeit oder Hitzebeständigkeit wurden bei der Entwicklung berücksichtigt. Somit kann der Anwender auch die übersetzte Applikation mit solch einem Dongle verschlüsseln und sie damit gegen sämtliche Formen von unberechtigter Vervielfältigung und Reverse Engineering schützen.

Schutz optionaler Funktionen

Benötigt ein Anwender einen noch flexibleren Schutz, so kann er die Lizenzierungsmöglichkeit von »CodeMeter« nutzen. Damit können die be-

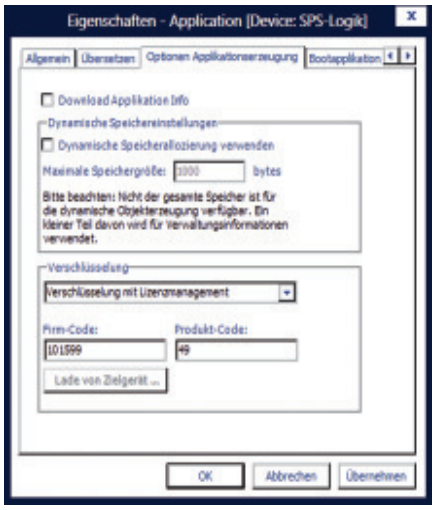
nötigten Lizenzen vom Anwender selbst erstellt und verwaltet werden. Zu diesem Zweck erwirbt er leere Dongles sowie einmalig einen Master-Dongle, die sogenannte »Firm Security Box« (FSB), mit der er selbst die gewünschten Parameter, zum Beispiel Product Code oder weitere Optionen wie Zähler oder Verfallsdaten, programmieren kann. Ganz automatisch verschlüsselt das Tool »AxProtector« die Anwendung.

Während der Security Key eine individuelle Anwendung schützt, kann der Hersteller mit seiner FSB eine Serienproduktion mit beispielsweise 100 identischen Steuerungen realisieren. Die Lizenzen werden hier also funktionsspezifisch vergeben anstelle spezifisch für eine Steuerung. Der Vorteil dabe ist, dass jeder Kunde die in Serie produzierte Maschine mit der identischen Steuerung erhält. Nur über die Lizenz im Dongle wird festgelegt, welche Funktionen der Kunde nutzen kann. Dazu kann der Applikationsprogrammierer mithilfe einer mitgelieferten Bibliothek im IEC 61131-3-Code die verfügbaren Lizenzinformationen abfragen und abhängig davon beispielsweise bestimmte Funktionen freischalten. Eine weitere Bibliotheksfunktion ermöglicht ihm darüber hinaus, sogar schützenswerte Daten innerhalb der Applikation so abzulegen und zu verschlüsseln, dass sie beispielsweise während einer Wartung des Quellcodes nicht im Klartext ausgelesen werden können.

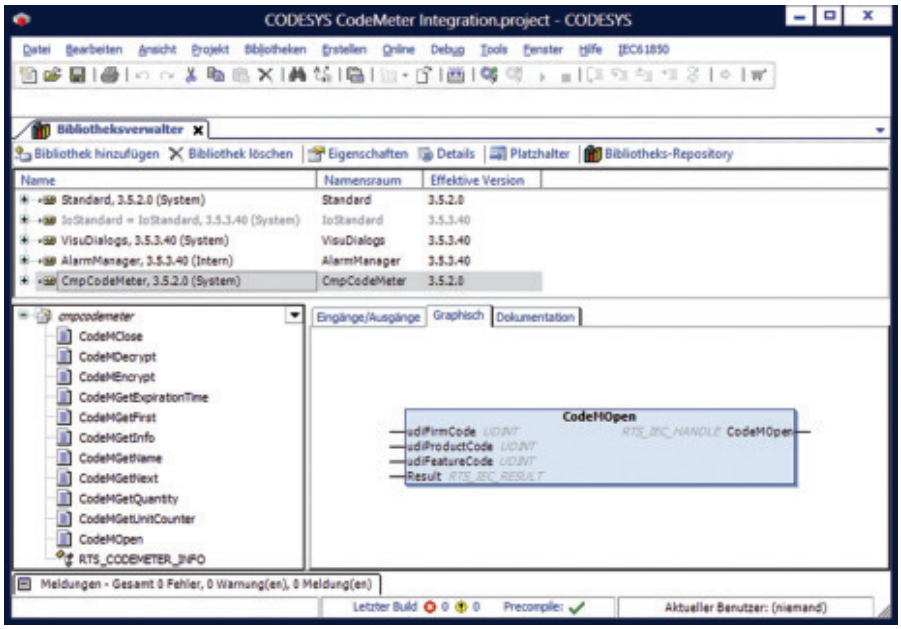
Auch 3S nutzt »CodeMeter« für die Lizenzierung von Zusatzfunktionen des »Codesys«-Entwicklungssystems. Die IEC 61131-3-Plattform kann als .NET-basiertes System durch Plug-in-Komponenten erweitert werden. Das System ist zwar bereits mit umfassenden Programmier- und Inbetriebnahmefunktionen ausgestattet, spezielle Zusatztools zur Produktivitätssteigerung bei der Applikationsentwicklung sind aber nicht für alle Anwender gleichermaßen attraktiv und deshalb nicht im Standardumfang enthalten. Möchten zum Beispiel Software-Entwickler mit Hochsprachenaffinität zusätzliche integrierte Tools nutzen, so finden sie entsprechende Optionen im Store. In diesem Online-App-Shop werden Plug-ins für UML, statische Code-Analyse, Profiling, SubVersion-Anbindung oder automatisierte Tests des Quellcodes angeboten, darüber hinaus kostenpflichtige Bibliotheken und viele kostenlose Beispiele. Die Anwender profitieren dabei wiederum von der nahtlosen Integration der »CodeMeter«-Technologie: Die Installation einer Zusatzkomponente kann direkt in der Entwicklungsumgebung erfolgen, eine erworbene Produktlizenz kann sofort in verbundene Security Keys hinterlegt werden. Abhängig vom Softwareprodukt ist dabei auch eine Lizenzierung pro Steuerung auf dem Dongle oder in einem verschlüsselten Software-Container möglich.

Der Anwender erhält zur Lizenzierung ein sogenanntes Ticket mit einer eindeutigen Identifikationskennzeichnung, quasi als Platzhalter für seine Lizenzen. Auf einem Lizenzserver ist vermerkt, welche Lizenzen im Ticket enthalten sind. Bei der Aktivierung von Lizenzen wird eine Verbindung zum Lizenzserver aufgebaut, die Lizenz abgebucht und auf den Dongle übertragen. Falls am »Codesys«-Arbeitsplatzrechner vor Ort keine Internetverbindung besteht, kann diese Lizenzierung auch zweistufig über ein dateibasiertes Handshake-Verfahren erfolgen. Der Lizenzierungsmechanismus kann von Anwendern und Geräteherstellern auch für eigene optionale Zusatzkomponenten genutzt werden: entweder über den Store oder aber über einen eigenen Lizenzierungsserver.

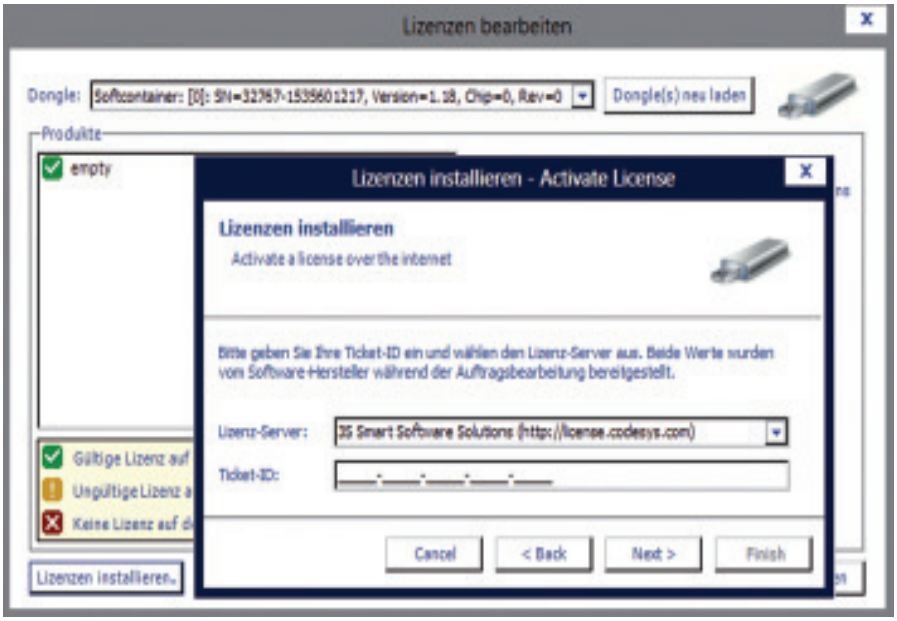
Insbesondere die Entwicklungen um Industrie 4.0 und Industrial Internet of Things (IIoT) stärken das Bewusstsein dafür, dass Intelligenz in Maschinen und Anlagen geschützt werden muss. Aufgrund der Einbettung der »CodeMeter«-Technologie in der IEC 61131-3-Plattform profitieren »Codesys«-Anwender von Maßnahmen, die einen höchstmöglichen Schutz geistigen Eigentums gewährleisten. Wie in anderen Bereichen des Lebens ist ein solcher Schutz mit einem gewissen Aufwand und Komfortverlust verbunden. Die nahtlose Integration zweier Technologien reduziert jedoch diese Einschränkungen und ermöglicht es dem Anwender, sein Knowhow mit eleganten Mitteln abzusichern.



Verschlüsselung der Bootapplikation per CmDongle. ***Screenshots: 3s***



IEC 61131-3-Bibliotheksbaustein zum Auslesen von Lizenzinformationen in der Applikation.



Aktivierung von optionalen Lizenzen direkt im »Codesys«-Entwicklungssystem.