White Paper

CodeMeter in der Automatisierungsindustrie

Win-Win-Situation für Steuerungshersteller und Maschinenbauer

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

WIBU SYSTEMS

Inhalt

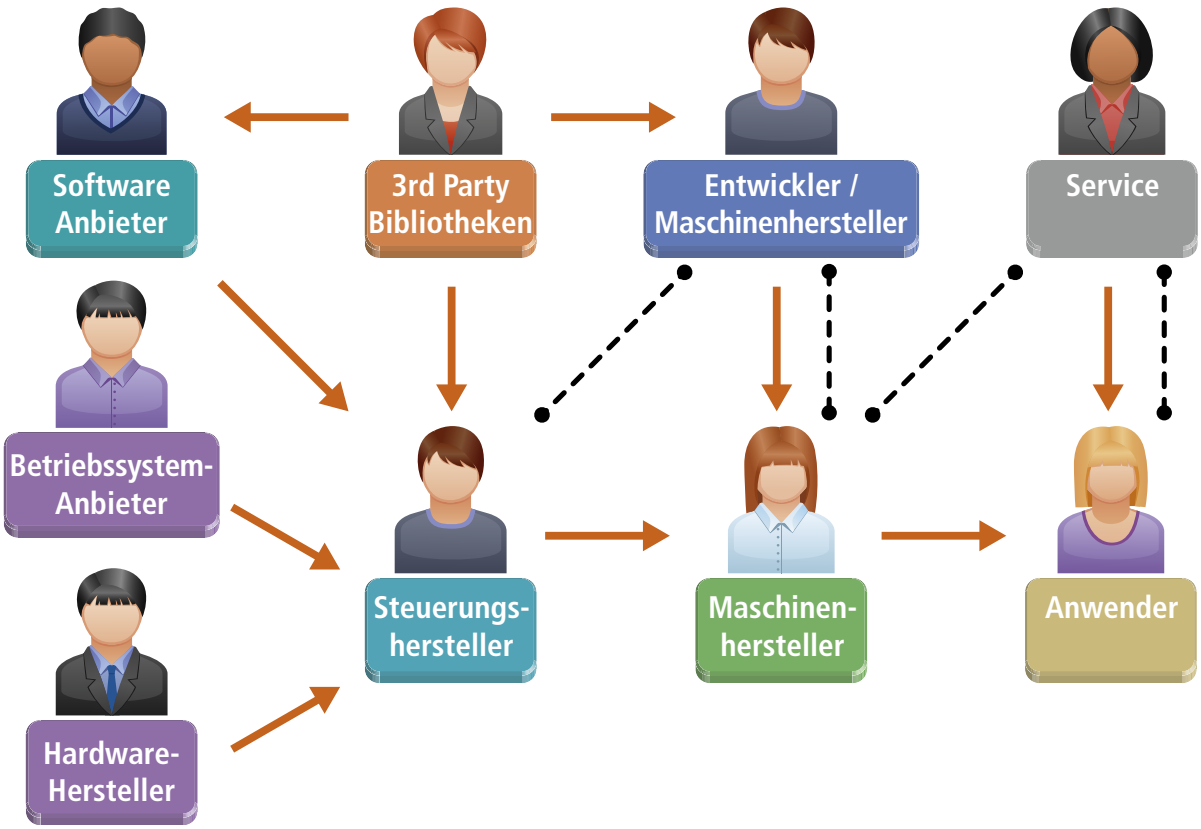
Einleitung

Maschinen, Anlagen und Geräte enthalten fast immer eine oder mehrere Steuerungen. Steuerungen bestehen typischerweise aus einer Kombination von Hard- und Software. Der Maschinenbauer programmiert darauf seine Anwendung. Software ist insgesamt ein wichtiges Alleinstellungsmerkmal für Maschinenbauer und Steuerungshersteller, denn viele Funktionen lassen sich erst durch ihren Einsatz umsetzen. Dieses Whitepaper beschreibt, welche Wettbewerbsvorteile Steuerungshersteller, Maschinenbauer und Maschinenanwender durch den Einsatz von CodeMeter erlangen können. Es stellt Funktions- und Anwendungsweise von CodeMeter und der generellen AxProtector-Technologie vor. Maschinenbauer sind kostenbewusst und hinterfragen die Preise für Steuerungen kritisch. Auch wenn ihre Maschinen insgesamt viel Geld kosten, der Preis für die eingesetzten Steuerungen darf dennoch nicht beliebig steigen. Der Einbau einer Sicherheitstechnologie wie CodeMeter kostet zunächst einmal Geld. Lohnen sich diese zusätzlichen Ausgaben? Wie hoch ist der Anteil der Steuerung an den Gesamtkosten einer Maschine und welchen Einfluss hätte eine Schutzfunktion innerhalb der Steuerung auf das langfristige Geschäft des Maschinenbauers?

Welche Vorteile impliziert ein Schutzsystem?

Verhindert beispielsweise der Einbau von Sicherheitstechnologie den Nachbau einer Maschine oder den kriminellen Wissenstransfer zur Konkurrenz, dann relativieren sich die Aufwendungen sehr schnell und wenige zusätzliche Euros wenden einen Millionenschaden ab. Gleichzeitig versetzt CodeMeter sowohl den Steuerungshersteller als auch den Maschinenbauer in die Lage, neue Geschäftsmodelle auf den Markt zu bringen und ihre Angebote mit minimalem Aufwand zu erweitern. Hier einige Beispiele von vielen: Fein abgestufte Lizenzen regeln die Nutzungsrechte einzelner Funktionen oder geben den Zugriff für einen befristeten Zeitraum frei. Features on Demand erfüllen Kundenwünsche und dabei kann der Hersteller seine Modellvielfalt kleinhalten. Der Schutz gegen Reverse Engineering verhindert den Nachbau, sichert Marktanteile und Renommee. Selbst der Betreiber einer Maschine oder Anlage profitiert davon. Der eingebaute Integritätsschutz verhindert Sabotage und Manipulation auf Softwareebene. Genauso denkbar wäre eine Fertigung, bei der die Produktionsmenge auftragsbezogen limitiert werden kann. Diese Begrenzung der Losgröße könnte ein Anlagenbetreiber als Zusatzleistung seinen Kunden anbieten. Dieser Kunde wäre geschützt vor einer Schwarzfertigung seiner Luxusartikel oder -textilien. Steuerungshersteller, Maschinenbauer und Anwender profitieren vom frühzeitigen, konsequenten Einbau von CodeMeter. Aber nur der Steuerungshersteller kann diese Win-win-Situation herbeiführen. Mit nur einem einzigen Produkt bekommt man die geschilderten Bedrohungsszenarien in den Griff und ebnet den Weg für neue Geschäftsmodelle. Eine klare Motivation für Steuerungshersteller, CodeMeter in ihre Steuerungen einzubinden und starke Argumente für ihre Verhandlungen mit Maschinenbauern.

In der Automatisierung gibt es unterschiedliche Beteiligte



Das Fundament der Sicherheit

Security fängt ganz unten im Entstehungsprozess einer Anlage oder Maschine an. Die einzelnen Bausteine sind dabei:

Steuerung und Entwicklungsumgebung

Setzt der Maschinenbauer für seine Anlage eine Steuerung ein, liefert der Steuerungsanbieter ihm zunächst eine Entwicklungsumgebung. Jeder Entwickler des Maschinenbauers, der an dem Projekt arbeitet, braucht dabei seine eigene Entwicklungsumgebung. Die Entwicklungsumgebung ist eine Softwarekomponente des Steuerungsherstellers. Es liegt im Interesse des Steuerungsherstellers, dass der Maschinenbauer für jeden seiner Entwickler die entsprechenden Lizenzen für die Entwicklungsumgebung erwirbt. Die Maschine selbst kann eine oder mehrere Steuerungen enthalten. Das Paket des Steuerungsanbieters besteht also aus Entwicklungsumgebungen und Steuerungen.

Hardware, Laufzeitumgebung und Betriebssystem

Eine Steuerung besteht prinzipiell aus Hardware und einer Laufzeitumgebung. Häufig kommen Betriebssysteme wie Windows Embedded, Embedded Linux oder das Echtzeitbetriebssystem VxWorks zum Einsatz, unter denen die Laufzeitumgebung ausgeführt wird. Es gibt aber auch Laufzeitumgebungen, die ohne Betriebssystem auskommen.

Die Laufzeitumgebung ist ebenfalls eine Softwarekomponente des Steuerungsherstellers. Sie enthält sein Know-how und ist eine entscheidende – und damit schützenswerte – Komponente seines Geschäfts.

IEC 61131 Sprache und Anwendung

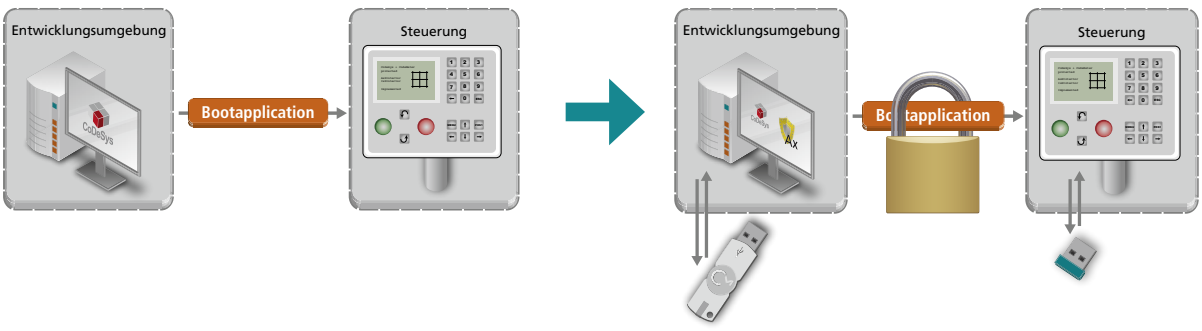
Der Maschinenbauer verwendet die Entwicklungsumgebung des Steuerungsanbieters, meist um in einer IEC 61131 Sprache seine Anwendung zu schreiben. Die Anwendung gibt der Steuerung die Anweisungen, wie sie die Aufgaben in der Maschine zu erfüllen hat. Das Know-how des Maschinenbauers liegt im Zusammenspiel aus Maschinenbau und Anwendung. Die Art, wie Sensoren, Motoren und Achsen zusammenspielen, entscheidet darüber, wie schnell und präzise die Maschine arbeitet. Die Leistungsfähigkeit seiner Maschine ist das Alleinstellungsmerkmal des Maschinenbauers. Sie ist das Ergebnis seiner Forschungen und Entwicklungen, insgesamt seiner Investitionen in F&E. Mit dem für F&E ausgegebenen Geld hält der Maschinenbauer seinen Entwicklungsvorsprung gegenüber seiner Konkurrenz. Ein überaus wertvolles und damit schützenswertes Kapital.

Schritt für Schritt zum Schutz mit CodeMeter

Betriebssystem, Laufzeitumgebung, Entwicklungsumgebung und Anwendung bauen aufeinander auf.

Entwicklungsumgebung schützt Anwendung mit AxProtector-Technologie

Im ersten Schritt verschlüsselt die Entwicklungsumgebung (IDE) mit der AxProtector-Technologie die Anwendung für die Übertragung zur Laufzeitumgebung. Man kann es sich mit dem folgenden Bild vorstellen: Die Entwicklungsumgebung „verschließt" die Anwendung in einer Kiste und versiegelt die Kiste mit einer „Unterschrift".



Durch den eingebauten AxProtector-Schutz läuft die Steuerung nur mit Lizenz im Dongle und vertifizierter Software

Ohne Schutz **Mit Schutz**

Laufzeitumgebung erhält geschützte Anwendung

Die Laufzeitumgebung auf der Steuerung erkennt, dass die Anwendung in einer verschlossenen Kiste übermittelt wurde. Sie weiß, wo sie den passenden Schlüssel zu dieser speziellen Kiste findet und wie sie diese Kiste aufschließen kann. Bevor sie die Kiste öffnet, prüft sie die Unterschrift, das Siegel. Ist die Unterschrift gültig, öffnet die Laufzeitumgebung mit ihrem Schlüssel die Kiste und entnimmt die Anwendung. Die Versiegelung gibt einen zusätzlichen Schutz gegen Saboteure. Unberechtigte Kisten mit Schadsoftware würden nicht ausgepackt. Ein Hacker hat durch die verschlüsselte Übertragung keine Chance, die Anwendung abzuhören. Die Anwendung wird mit der größtmöglichen Sicherheit von der Entwicklungsumgebung an die Laufzeitumgebung übermittelt.

Schutz der Laufzeitumgebung

Versucht der clevere Hacker die Laufzeitumgebung zu modifizieren, scheitert er auch hier an den Schutzmechanismen von CodeMeter. Es ist für den sicheren Schutz wichtig, dass die Laufzeitumgebung sicher gebootet wird. CodeMeter ist für viele Betriebssysteme und Laufzeitumgebungen verfügbar.

Fundament

Nur wenn in Betriebssystem, Laufzeitumgebung, Entwicklungsumgebung und Anwendung CodeMeter und die AxProtector-Technologie als Schutzsystem eingebaut sind, können alle Beteiligten dieser Kette ihr Kapital wirksam schützen. Der Vorteil von CodeMeter ist hierbei klar: Ein einziges Produkt reicht aus, um alle gemeinsam zu schützen. Dabei können Lizenzen alle Beteiligten auf nur einem Dongle untergebracht werden.

Die Bedrohungen und der Schutz dagegen:

Copy Cats durch Reverse Engineering

CC, genannt Copy Cat, war die erste geklonte Katze. Doch obwohl die Gene des Originals verwendet wurden, unterschied sich die Fellfarbe des geklonten Tieres von seiner Klonmutter. In global agierenden Märkten steigt die Zahl der Nachahmer. Davon sind alle Branchen betroffen. Hersteller von Industriegütern leiden darunter genauso wie Lieferanten von Luxusartikeln oder Designermoden. Die Plagiatoren sparen sich die Kosten für F&E, nutzen minderwertige Materialien und können damit erheblich günstiger anbieten. Sie zerstören und verunsichern Märkte. Oftmals werden die Nachbauten noch mit dem Namen des Originals angeboten. Bei mangelhafter Qualität des Plagiats ist der Schaden für das eigene Image erheblich. 100% Sicherheit gibt es nicht, doch man kann die Entstehung von Plagiaten erschweren. Wie geht ein Nachahmer vor? Er liest die verfügbaren Dokumente, wertet Prospekte, Datenblätter und Manuals aus. Er macht während einer Messe Fotos von dem Objekt seiner Begierde. Möglicherweise kauft er sich ein Produkt, um es auseinanderzunehmen und zu vermessen. All dies lässt sich nicht wirklich verhindern. Bei der Analyse der Software kann er hingegen massiv durch CodeMeter und die generelle AxProtector-Technologie gestoppt werden. Hier scheitert sein Versuch des Reverse Engineerings. Vorausgesetzt, auf allen Ebenen der Softwarekette ist CodeMeter und AxProtector-Technologie eingesetzt. Die geschützte Kette besteht aus Bootloader, Betriebssystem, Laufzeitumgebung, Anwendung, Parameter und Konfigurations- sowie Anwenderdaten. CodeMeter ist für viele Betriebssysteme und Laufzeitumgebungen verfügbar.

Mit AxProtector verschlüsselte Funktionen, Klassen und Methoden werden für den Hacker unlesbar

Schutz vor Reverse Engineering

Um eine Maschine nachbauen zu können, braucht man Zugang zu ihrer Software, der Anwendung. Ein Plagiator wird deshalb versuchen, die Anwendung von der Steuerung zu extrahieren und den Quellcode der Anwendung durch Reverse Engineering des Binärcodes zu gewinnen. Dies wird durch die AxProtector-Technologie verhindert oder extrem erschwert.

Lizenzschutz und Raubkopien

Kaufe eine, nutze viele. Nach diesem Motto wird Software oftmals behandelt.
Freche Zeitgenossen versorgen ihre Freunde mit Software oder treiben regen Handel mit fremdem Eigentum. CD kopieren und die einfache Lizenznummer abtippen, fertig ist die Raubkopie. Schnell sind dann viele SW-Pakete unter der gleichen Lizenznummer installiert. Einfache Lizenznummern und Passwörter sind kein wirksamer Schutz. Ein integrierter Lizenzschutz mit CodeMeter baut erheblich höhere Hürden für den Kriminellen auf. Professionelle Hacker sind bis heute an CodeMeter gescheitert. Der Return of Invest des Herstellers ist gesichert, weil sein Softwareprodukt nur mit einer gültigen Lizenz funktioniert. Die Kontrolle über die Lizenz behält er mit CodeMeter in der Hand. Die CodeMeter License Central ist der zentrale Verwaltungsplatz für die Erzeugung und Auslieferung der Lizenzen. Sie wird in Vertriebs- und Geschäftsprozesse integriert und vereinfacht die Logistik und Kontrolle für den Lizenzherausgeber. Lizenzschutz war früher auf PC-Software beschränkt. Doch Software ist heute in Maschinen und Anlagen ein wesentlicher Faktor. Viele Funktionen werden durch Software realisiert. Die Gefahren bestehen also auch in der Automatisierung.

Exportkontrolle

Steuerungen sind universell einsetzbare, leistungsfähige Elemente. Sie unterliegen häufig gesetzlichen Exportbeschränkungen. Der Steuerungshersteller muss nachweisen und sicherstellen, dass seine Produkte nicht in Embargoregionen zum Einsatz kommen. Der selektive und restriktive Verkauf an vertrauenswürdige Maschinenbauer in Verbindung mit CodeMeter-Lizenzschutz ist hierfür ein Weg. Die Lizenzrechte lassen sich bis auf einzelne Funktionen herunterbrechen. Ausgewählte, kritische Eigenschaften sind dann mit Lizenz versehen und funktionieren nur mit entsprechender Lizenz. Der Steuerungshersteller hält auf diese Weise seine gesetzlichen Vorgaben der Exportbeschränkung ein. Er kommt seiner Sorgfaltspflicht nach, denn die Verteilung der Lizenzen ist in CodeMeter License Central fälschungssicher dokumentiert. Der logistische Aufwand ist gering. Das gilt auch für den Erwerber der Lizenz. All seine Lizenzen liegen in nur einem Lizenzcontainer. Als Lizenzcontainer stehen Softlizenzen oder industrietaugliche Dongles zur Verfügung.

Terror, Sabotage

Terroranschläge und Sabotage sind reale Bedrohungen unserer Zeit. Cyberkriminalität nimmt ebenfalls zu. Zum klassischen Bombenbastler und Selbstmordattentäter kommt der smarte Kriminelle hinzu, der durch Manipulation von technischen Einrichtungen sein Ziel anstrebt. Sein Bestreben ist es, einen spektakulären und hohen Schaden anzurichten. Dabei ist es für den Erfolg des Attentäters egal, ob die Anlage durch eine Bombe oder durch eine fehlgeleitete Steuerung explodiert. Aus Habgier, Rache oder Fanatismus werden Mensch, Maschine und Produkt immer häufiger zu Zielen krimineller Machenschaften. Steuerungen sitzen überall. Die fahrerlose U-Bahn in der Großstadt enthält genauso Steuerungselemente wie die Chemieanlage oder das einsam gelegene Windkraftwerk. Fernwartung und Parametrierung übers Internet öffnen Cyberkriminellen Schlupflöcher, um auf Anlagen zugreifen zu können. Steuerungen befinden sich meistens in internen Netzwerken. Der Zugang zu diesen internen Netzwerken ist durch VPN und Firewall geschützt. Aber ist damit auch die Steuerung selbst vor unberechtigtem Zugriff sicher? Zugangsdaten zum VPN können gestohlen werden oder durch Erpressung in die Hände eines Angreifers gelangen. Auch eine Firewall ist für professionelle Hacker ein überwindbares Bollwerk. Befindet sich ein Angreifer durch seine Hackeraktivität erst einmal im internen Netzwerk, stehen ihm die meisten Türen offen. Hinter der Firewall im VPN hat er vollen Zugriff auf alle ungeschützten Steuerungen. CodeMeter verhindert den unbefugten Zugriff auf die Steuerungen. Jede einzelne Steuerung ist in sich geschützt. Auf eine Steuerung mit CodeMeter Schutz hat ein Hacker keinen Zugang. Er kann weder seine Schadsoftware auf die Steuerung laden, noch kann er sie anderweitig manipulieren.

Demogeräte

Ist der Terrorist besonders gewitzt, dann verschafft er sich Zugang zu den Entwicklungswerkzeugen oder Entwicklungsprototypen. Doch auch hier wird er an CodeMeter scheitern. Seine Analyse des Demogeräts versetzt ihn nicht in die Lage, das Livesystem zu manipulieren. Unterschiedliche Schlüsselkreise verhindern dies. Voll funktionsfähige Prototypen sind damit inkompatibel zum späteren realen System.

OPC UA mit Security

OPC UA ist ein Protokoll, mit dem herstellerunabhängig auf Geräte über das Internet zugegriffen werden kann. Fernwartung ist ein typischer Einsatzfall hierfür. Im OPC-UA-Standard gibt es eine Spezifikation für Security. Doch meistens wird OPC UA ohne Security angewendet. Denn in der Praxis liegt das Hauptproblem in der Verwaltung und Verteilung der Schlüssel und Berechtigungen. Das Problem der Zugangsschlüsselverwaltung wird von Wibu-Systems mit der CodeMeter License Central gelöst. Die CodeMeter License Central verteilt auch Zertifikate. CodeMeter kann in OPC UA hineinkonfiguriert werden. CodeMeter nutzt bei seiner Integration in OPC UA die Protokolle von OPC UA und ist damit konform zu diesem Standard. Damit steht OPC UA mit Security für Authentifizierung und verschlüsselte Kommunikation zur Verfügung.

Integritätsschutz

Der zuverlässige Integritätsschutz einer Anlage ist ein wichtiges Verkaufsargument. Ein weiterer Aspekt des Integritätsschutzes betrifft normenkonforme Komponenten. Branchenspezifische Normen regeln, welche Eigenschaften ein Gerät besitzen muss. Bahnzertifizierte, explosionsgeschützte, für Lebensmittel geeignete, vibrations- und wasserfeste Komponenten sind für ihren jeweiligen Zweck besonders ausgerüstet. Der Betreiber einer Anlage möchte natürlich sicher sein, dass er nur zugelassene Komponenten und seine eigene Software einsetzt. Dieser Integritätsschutz lässt sich mit CodeMeter durch signierten Programmcode und Prüfung gegen eine Zertifikatskette einbauen.

Manipulation

Jedes technische Gerät ist für einen spezifizierten Betriebsbereich gebaut. Der Hersteller garantiert für einen reibungslosen Betrieb innerhalb dieser Spezifikation. Welche Konsequenzen hat es für den Hersteller, wenn sein Kunde Geräte und Anlagen nach eigenem Gutdünken tuned, um eine höhere Leistung „herauszukitzeln“ und dabei den spezifizierten Bereich verlässt? Ein „frisiertes“ Motorrad fährt schneller, knattert lauter und wird von der Polizei früher oder später aus dem Verkehr gezogen. Der Fahrer verliert seinen Versicherungsschutz und zahlt Strafe. Eine „frisierte“ Anlage läuft möglicherweise auch schneller und erwirtschaftet dem Betreiber eine höhere Rendite. Doch ihre Komponenten verschleißen ebenfalls in Rekordtempo. Kann der Hersteller seinem Kunden den Betrieb außerhalb der Spezifikation nicht nachweisen, dann kostet es ihn Geld für Gewährleistung und Serviceeinsätze. Mit CodeMeter kann der Hersteller sich vor unbefugtem Verändern von Parametern schützen oder diese Veränderung fälschungssicher in einem Logbuch dokumentieren.

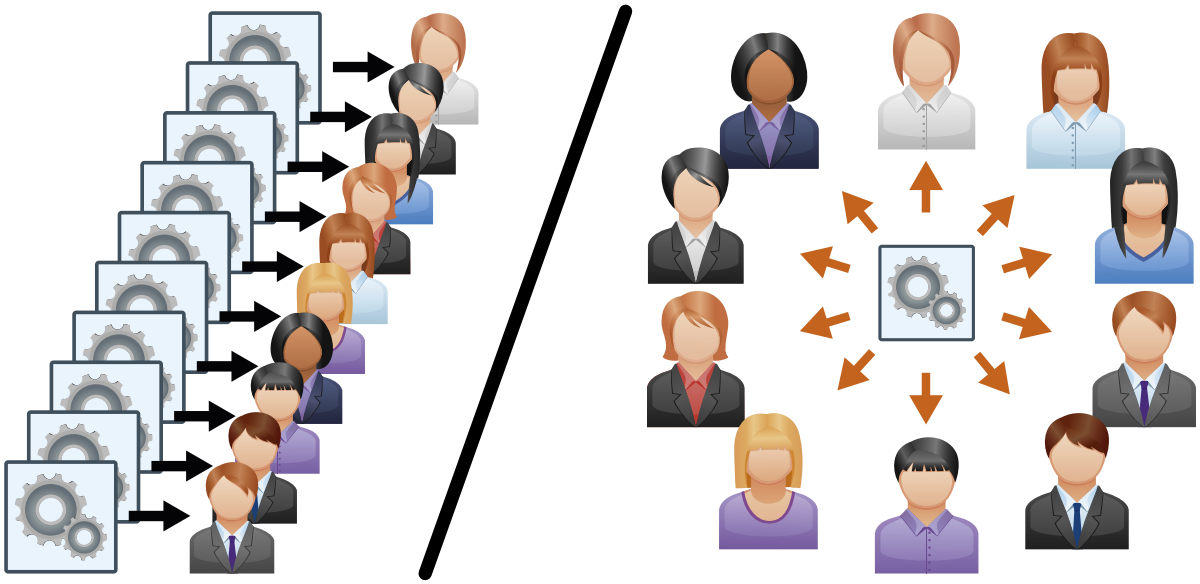
Modularer Schutz des Quellcodes des Maschinenbauers

Der lesbare Quellcode der Anwendung liegt beim Maschinenbauer. Es kommt vor, dass seine Kunden darauf bestehen, den Quellcode für ihre Anlage zu bekommen. Dann ist ein funktionierender Schutz dieses Quellcodes besonders wichtig. Der Kunde kann mit dem Besitz des Quellcodes in die Funktion der Maschine eingreifen. Ein Editieren des Quellcodes durch geschultes Servicepersonal des Kunden mag in Einzelfällen durchaus sinnvoll sein. So könnte beispielsweise ein weniger relevanter, defekter Sensor aus der weiteren Berücksichtigung genommen werden, damit die Produktion bis zur Reparatur der Maschine weiter läuft. Sicherheitskritische und Kern-Know-how enthaltende Teile müssen hingegen vor dem Zugriff geschützt liegen. CodeMeter ist für eine fein abgestufte Berechtigung bestens gerüstet. Der Kunde darf zudem nicht in die Lage versetzt werden, einen funktionsfähigen Quellcode an ungefugte Dritte weitergeben zu können. Auch hier setzen die Lizenzierungsmechanismen von CodeMeter einen Riegel vor. Neben Kunden gibt es auch Mitarbeiter, die Zugang zum Quellcode haben. Die Entwickler des Maschinenbauers haben mit einer IEC 61131 Sprache die Anwendung geschrieben. Sie haben Zugang zum lesbaren Quellcode. Der Servicetechniker muss möglicherweise bei seinen Arbeitseinsätzen mit dem Quellcode arbeiten. Ein krimineller Plagiator könnte durch Erpressung oder Bestechung an diese Mitarbeiter herantreten, um an den Quellcode zu kommen. Der Quellcode muss gegen untreue Mitarbeiter und illoyale Kunden gleichermaßen geschützt werden. Diesen Schutz gewährt CodeMeter. Dann liegt dem Plagiator zwar der lesbare Quellcode vor, doch er kann keine lauffähige Anwendung daraus erzeugen.

Neue Geschäftsmodelle

Produktionskosten reduzieren

Produktionskosten lassen sich senken, wenn mehrere Leistungsvarianten mit nur einem Produkt abgedeckt werden können. Zusätzlich sinken die Kosten für die Produktpflege. Software eignet sich optimal für dieses Modell. Vorausgesetzt, der Hersteller kann seine Leistungsvarianten vor unbefugter Nutzung schützen. Eine Software steuert beispielsweise eine beliebige Anzahl Achsen. Doch ein Maschinenbauer, der nur zwei Achsen steuern muss, möchte auch nur für die Funktion „zwei Achsen" zahlen. Dabei ist es dem Maschinenbauer egal, ob die Steuerung theoretisch acht Achsen steuern kann. In unserem Beispiel liefert der Steuerungshersteller dem Maschinenbauer seine Steuerungssoftware mit der Fähigkeit für acht Achsen. Die mitgelieferte Lizenz schaltet aber nur die Bedienung von zwei Achsen frei. Die Abwicklung und Verwaltung der Lizenzierung erledigt der Steuerungshersteller mit der CodeMeter License Central. Mit den Lizenzierungsmöglichkeiten von CodeMeter ist der Steuerungshersteller in der Lage, jede Art von fein abgestufter Berechtigung in sein Produkt einzudesignen. Damit behält er weiterhin nur ein Produkt in der Pflege und kann für jeden Bedarf die passenden Berechtigungen lizenzieren. Ein schlanker Produktionsprozess ist die Folge. Der Aufwand für die damit verbundene Lizenzlogistik ist mit CodeMeter License Central gering.



Einfachere Logistik: Anstatt 10 individuelle Maschinen für 10 Kunden gibt es nur noch eine Maschine die alles kann und mittels Lizenzen konfiguriert wird.

Features on Demand

Möglicherweise stellt der Maschinenbauer im Laufe der Entwicklung fest, dass er mit seiner neuen Steuerung noch vier weitere Achsen bedienen möchte. Er kauft zusätzliche Lizenzen, aktiviert sie in seiner bestehenden Software und steuert die weiteren Achsen mit den freigeschalteten Funktionen an. Hierzu muss keine neue Software installiert werden. Der Steuerungshersteller reagiert flexibel auf die Wünsche seines Kunden und liefert eine individuell skalierte Lösung, die auf seinem generellen Produkt basiert. Genauso kann der Maschinenhersteller seinem Kunden in der bereits gekauften und installierten Maschine zusätzliche Funktionen freischalten und berechnen. Neues Geschäftspotenzial entsteht.

Zeitlich begrenzte Lizenzen

Manche Software will man einfach einmal ausprobieren, um Eigenschaften kennenzulernen oder Benchmarks zu fahren. Der Anwender möchte dazu am liebsten die Vollversion der Software testen. Dann muss der Hersteller sicherstellen, dass aus der gelieferten Demo-Vollversion nicht heimlich eine Dauerversion wird. Zeitlich limitierte Lizenzen sind hierzu die Lösung. Zeit- oder Mengen beschränkende und funktionsbezogene Lizenzen lassen sich kombinieren.

Servicetechniker an der kontrollierten Leine

Zeit- oder Mengenbeschränkende Lizenzen sind auch für Installations-, Wartungs- und Reparaturleistungen interessant. Ein Servicetechniker erhält für seine Arbeit meistens sehr weitreichende Berechtigungen. Aus Sicherheitsgründen ist es sinnvoll, diese auf die Dauer seines Einsatzes beim Kunden zu begrenzen. Damit kann der Mitarbeiter die Arbeiten erledigen. Die Lizenz erlischt nach der Durchführung und ist für unbefugte Hände wertlos.

Mengenbeschränkende Lizenzen

Die Anzahl der Zugriffe zu einer Funktion oder zur Software insgesamt kann limitiert werden. Auch der Maschinenbauer könnte mit limitierenden Lizenzen zusätzliches Geschäft initiieren. Mit der Mengenbeschränkung könnte beispielsweise eine Fertigungsvorlage nach einer definierten Losgröße gesperrt werden. Damit verhindert die Maschine, dass auf ihr in einer illegalen Nachtschicht beispielsweise teure Designermoden zugeschnitten werden, die Kriminelle danach im Hinterzimmer nähen und über dunkle Kanäle in den Handel bringen.

Nachrüsten von Steuerungen

Nicht jede Steuerung ist heute bereits mit CodeMeter-Funktionen ausgestattet. Eine Nachrüstung in bestehende, gelieferte Maschinen ist jedoch technisch möglich. Die Wibu-Systems-Dongles sind industrietauglich, und für viele verschiedene Schnittstellen erhältlich. Dazu gehören CmSticks als USB-Dongles genauso wie CmCards als SD Card, microSD Card oder CompactFlash Card. Die robusten Sticks und Cards arbeiten stabil über einen erweiterten Temperaturbereich und sind gegen Kondenswasser durch ein Conformal Coating geschützt. Lizenzen für CmDongles oder CmActLicense-Dateien mit Aktivierungen für die Steuerung können an die Steuerung online oder offline übertragen werden. Dies ist vor allem für Maschinen ohne Internetzugang interessant.

Zusammenfassung

Nur der Steuerungshersteller kann die Win-Win-Situation für die nachgeschalteten Partner durch den Einbau von CodeMeter und der AxProtector-Technologie herbeiführen. Die Basis ist vorhanden, weil der CodeMeter-Schutz bereits für viele Betriebssysteme verfügbar ist und beispielsweise auch in Steuerungssystemen wie CODESYS oder Automation Studio von Bernecker & Rainer integriert ist.

Entscheidet sich der Steuerungshersteller für den Einbau, gewinnen er und seine Partner folgende Vorteile:

- Schutz gegen Reverse Engineering
- Schutz vor Raubkopie und Nachbau
- Neue Geschäftsmöglichkeiten durch Features on Demand
- Verbesserte Exportkontrolle
- Integritäts- und Manipulationsschutz
- Fälschungssicheres Logbuch
- Schutz vor Sabotage
- Kontrolle von Demogeräten
- Vereinfachte Logistik für Maschinen durch Softwarelizenzierung
- Geringere Produktionskosten
- Sicherung des Entwicklungsvorsprungs und der F&E-Investitionen

Es ist möglich, den Schutz in Steuerungen durch Software-Updates nachzurüsten. Der Weg zu Berechtigungen, Zertifikaten, Schlüsseln und Lizenzen ist mit CodeMeter einheitlich. CodeMeter ist eine skalierbare Lösung und deckt alle beschriebenen Einsatzfälle ab. Die CodeMeter-Lizenzen sind in einem Lizenzcontainer, beispielsweise einem Dongle oder einer Lizenzdatei, untergebracht. Das gilt auch für Rechte mehrerer Rechteinhaber, also Steuerungshersteller, Maschinenhersteller und Produktionsauftraggeber. Die CodeMeter-Dongles von Wibu-Systems sind industrietauglich.

Autor:
Oliver Winzenried ist begeisterungsfähiger Verfechter von Sicherheitslösungen, die gepaart mit innovativen Technologien das geistige Eigentum und Umsätze unabhängiger Software-Hersteller schützen. Unmittelbar nach Abschluss seines Elektrotechnikstudiums an der Universität Karlsruhe begann er seine unternehmerische Laufbahn in der Entwicklung von Elektronik- und ASIC-Bausteinen, Hardware, Mikrocontroller und Eingebetteter Systeme für die Bereiche Unterhaltungselektronik, Automobil- und Betriebstechnik. In 1989 gründete er zusammen mit Marcellus Buchheit die WIBU-SYSTEMS AG, deren Geschäftsführer er seitdem ist. Seine Leidenschaft für den Integritätsschutz von Software findet ihren Ausdruck in zahlreichen Patenten, die vom sicheren Lizenzmanagement bis zu Produktinnovationen bei Dongles reichen. Als Autor liefert er regelmäßig Beiträge zu Leitartikeln und Büchern und seine Vorträge finden die Aufmerksamkeit auf großen Messen, Ausstellungen, Konferenzen, Industrieverbandsveranstaltungen und Technologiezentren wie das Fraunhofer Institut. Sein persönliches Engagement in internationalen Projekten im F&E-Bereich und Standardisierungsgremien, wie z. B. die SD Card Association, runden sein Profil ab. Oliver Winzenried ist überdies Vorstandsvorsitzender der Arbeitsgemeinschaft Produkt- und Know-how-Schutz „Protect-Ing“ des VDMA, im Hauptvorstand der BITKOM sowie im Vorstand des Fördervereins Forschungszentrum Informatik FZI am KIT.

Kontakt:
WIBU-SYSTEMS AG
Tel.: +49-721-93172-0
Fax: +49-721-93172-22
E-Mail: info@wibu.com

www.wibu.com

5062-003-01/20132409

WIBU-SYSTEMS AG (WIBU®) wurde 1989 von Oliver Winzenried und Marcellus Buchheit gegründet. Seit dem ersten Auftreten revolutioniert Wibu-Systems die internationale Szene mit sicherheitstechnologischer Innovation. Die Lösungen des Portfolios schützen digitale Produkte, geistige Eigentumsrechte und die Integrität digitaler Daten vor Software-Piraterie, Nachkonstruktion und Quellcode-Manipulation. Die breite und vielfach ausgezeichnete Palette von Wibu-Systems-Lösungen ist einzigartig und umfasst die Anwendungsbereiche von Rechnern zu Mobiltelefonen, von eingebetteter Automatisierung zum Cloud Computing, von SaaS zu virtuellen Modellen.

Durch das Motto „Perfection in Protection“ hat Wibu-Systems neue Geschäftsmodelle eröffnet; Software-Anbieter, ob im Konsumenten-, Unternehmens- oder Embedded-Bereich, können über abgestimmte Lizenzierungsstrategien Erlöse aus ihrem Invest erzielen.
Mit Sitz in Karlsruhe unterhält Wibu-Systems Niederlassungen in Seattle (USA) sowie Schanghai und Peking (China), Verkaufsbüros in Belgien, Frankreich, Großbritannien, den Niederlanden, Portugal und Spanien sowie ein engmaschiges, weltweites Netzwerk an Distributoren.

20+ Years
MEDIA ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU SYSTEMS