Industrie 4.0 meets Security

01 Die Schutzhardware „CmDongle" von Wibu-Systems erfüllt industrielle Anforderungen

Ende letzten Jahres wurde die Online-Landkarte der Plattform Industrie 4.0 mit Praxisbeispielen zum Thema Industrie 4.0 vorgestellt. Mit dabei ist auch das Projekt „Codemeter zum Schutz von Know-how und Produktionsdaten" von Wibu-Systems. Die Schutztechnologie unterstützt unter anderem Maschinenhersteller in der Textilindustrie, ihre Maschinen vor Spionage und Sabotage zu schützen. Ebenso kommt sie Auftraggebern von Textilproduktionen zugute, die damit ihre Produktionsdaten schützen können.

02 Wertvolles Know-how und Algorithmen in der Produktion müssen vor Produktpiraten, Wirtschaftsspionen und Saboteuren geschützt werden

03 Stickmaschine von hinten: Die Schutzhardware „CmDongle" steckt auf einer Stickmaschine und schützt, lizenziert und verhindert Manipulationen

Zu den Kriterien eines funktionierenden und erfolgreichen Industrie-4.0-Konzepts zählt der Schutz von Embedded-Software und von Produktionsdaten. In der Vergangenheit wurde die Fabrik mit Fabrikzäunen, Alarmanlagen und Wachpersonal ausreichend geschützt. Für die intelligente Fabrik reicht dies nicht mehr aus: Wirtschaftsspione, Produktpiraten oder Saboteure entwickeln immer raffiniertere Cyber-Angriffe. Sie nutzen PC und Internetverbindungen, um ins Produktionsnetzwerk einzudringen. Ein Schutzkonzept ist nur geeignet, wenn es Cyber-Angriffe identifiziert und verhindert und das Know-how in Maschinen, Anlagen und Geräten vor Diebstahl und Manipulation schützt.
Mit einem geeigneten technisch-präventiven Schutz können Hersteller ihre Embedded-Software verschlüsseln und signieren, um Produktpiraterie und Manipulation zu verhindern. Dieser Schutz muss einen hohen Sicherheitslevel bieten, für den Einsatz in der Industrie geeignet sein und modernen Anforderungen der intelligenten Produktion wie der wachsenden Vernetzung im Sinne von Industrie 4.0 entsprechen. Produkte, Daten, Know-how und sensible Produktionsnetze sind besonders schützenswert. Das Schutzkonzept muss das Eindringen von Produktpiraten, Wirtschaftsspionen oder Saboteuren verhindern, damit das Expertenwissen innerhalb der Unternehmensmauern bleibt. Zusätzlich müssen die Produktionsprozesse ungestört ablaufen und fehlerhafte Produktion oder sogar Beschädigungen der Maschinen verhindert werden.
Die Wibu-Systems AG hat dazu die Schutztechnologie Codemeter entwickelt. Sie erfüllt unterschiedliche Sicherheitsbedürfnisse der Industrie, einschließlich moderner Security-Maßnahmen für Industrie 4.0 und das Internet der Dinge. Das Konzept beruht auf der Ver- und Entschlüsselung der Embedded-Software mit der sicheren Speicherung von „Schlüsseln". Zusätzlich wird der Programmcode vor Manipulation durch den Einsatz von elektronisch signiertem Code und der Prüfung gegen eine Zertifikatskette geschützt. Die Einsatzmöglichkeiten von Codemeter sind vielfältig: Sie erlauben „Protection", also den Schutz gegen Kopieren und Reverse-Engineering; „Licensing", das neue Geschäftsmodelle durch flexible Funktionsfreischaltung und Integration in den Vertriebsprozess ermöglicht; sowie „Security", das heißt Schutz vor Manipulation und Cyber-Angriffen.

Das Schützenswerte einer Stickmaschine
Eingesetzt wird die Codemeter-Technologie beispielsweise bei einem Maschinenhersteller in der Textilindustrie (Bild 2 und Bild 3). Dort schützt sie zum einen die Maschine selbst vor unberechtigtem Nachbau und Reverse-Engineering. Zum anderen werden damit die Produktionsdaten der Auftraggeber von Textilproduktionen gesichert, die auf diesen Maschinen in externen Fabriken produzieren lassen. Insgesamt lässt sich auf diese Weise aber nicht nur die unberechtigte Nutzung der Produktionsdaten verhindern, sondern auch die Produktionsstückzahl kontrollieren und damit die unbemerkte Herstellung von „Originalprodukten" für den Graumarkt ausschließen.
In der Textilproduktion, die nach den Gesichtspunkten der Industrie 4.0 aufgebaut ist, sind die einzelnen Stickmaschinen miteinander vernetzt und tauschen sich untereinander aus. Sobald eine Maschine ihren Stickauftrag

abgearbeitet hat, meldet sie ihren Status an das dazugehörige Maschinenkollektiv. Dabei muss das System so sicher sein, dass mögliche Saboteure bei Manipulationsversuchen gestoppt werden und die Embedded-Software jederzeit sicher funktioniert. Das bedeutet, dass die Integrität der Embedded-Software gewährleistet sein muss. Codemeter entspricht dem, indem es die Embedded-Software digital signiert. Nur die korrekt signierten Programmteile werden vom Schutzsystem entschlüsselt und ausgeführt. Passt die Signatur nicht, wird die manipulierte Software nicht ausgeführt und ein möglicher Schaden verhindert.
Durch die Verschlüsselung der Steuerungssoftware verhindert der Hersteller, dass Produktpiraten das Know-how in dieser Software analysieren oder unberechtigt benutzen können. Auf diese Weise wird der Nachbau der Stickmaschine verhindert. Zusätzlich sind intelligente Verfahren und Algorithmen der Software weiterhin geheim; der Hersteller kann seinen Wettbewerbsvorsprung halten.
Darüber hinaus kommt dem Schutz der Dokumente große Bedeutung zu. So enthalten technische Zeichnungen oder Serviceunterlagen wertvolle Details, das heißt schützenswertes Know-how. Mit Codemeter kann der Hersteller die PDF-Dokumente verschlüsseln, sodass nur Berechtigte diese mit der passenden Berechtigung in ihrem Schlüssel lesen können, wahlweise zeitlich oder funktionell begrenzt.
Neben diesen Schutzmöglichkeiten sichert die Codemeter-Technologie auch die Produktionsdaten. Das ist vor dem Hintergrund wichtig, dass der Betreiber der Stickmaschine die Originaldaten vom Auftraggeber erhält und damit die gewünschten Produktionsaufträge abarbeitet. Die Gefahr bei ungeschützten Produktionsdaten ist, dass der Betreiber theoretisch in einer Nacht- oder Sonderschicht mit diesen Originaldaten weiterproduzieren und die so produzierten Markenprodukte als Plagiate in hochwertiger Qualität für den Graumarkt verkaufen könnte. Mittels eines Zählers, der die zu produzierende Stückzahl definiert, schützt Codemeter die Produktionsdaten. Nur der Auftraggeber kann den Zähler für den nächsten Produktionsauftrag wieder hochsetzen. Somit sind beide Parteien auf der sicheren Seite.
Außerdem erlaubt Codemeter dem Hersteller, all die unterschiedlichen Funktionen seiner Embedded-Software unterschiedlich zu verschlüsseln und zu lizenzieren, sodass der Käufer nur die entsprechenden Funktionen nutzen kann. Nachträglich sind weitere Funktionen jederzeit freischaltbar und so zusätzliche Verkäufe realisierbar. Auf diese Weise kann der Hersteller die Funktionen seiner Stickmaschine verkaufen und die Nutzungszeit abrechnen oder die ganze Maschine vermieten. Im Falle von Wartung oder Reparatur schickt der Hersteller seine Servicetechniker zur Maschine. Die für den Einsatz notwendigen Zusatzfunktionen oder PDF-Dokumente werden für den geplanten Zeitraum freigeschaltet. Auch Softwarehersteller, die PC-basierte I Designsoftware für die Erstellung der Punch-Daten oder Stickmuster anbieten, schützen ihre Steuerungssoftware vor Kopieren und können die Software nutzungsgenau abrechnen.

Technische Details
Codemeter ist auf den gängigen Betriebssystemen Windows, Mac OS und Linux einsetzbar, aber auch auf den industrietypischen Systemen, wie Windows Embedded, Real Time Linux und „VxWorks“, sowie SPS-Umgebungen, wie Codesys oder der Steuerung von B&R. Sowohl klassische PC-Software als auch Embedded-Software, Betriebssystem-Images oder Maschinendaten können geschützt werden.
Die Schutzhardware (Bild 1) als Träger der Nutzungsrechte gibt es für die USB-Schnittstelle und für die industriellen Schnittstellen, wie „CFast“, „microSD“, SD und CF mit erweitertem Temperaturbereich und SLC-Flash. Mit der Schutztechnologie lassen sich auch programmierbare Logikbausteine oder Mikrocontroller schützen. Zusätzlich zeichnet sich die Schutzhardware durch gute EMV-Eigenschaften, Feuchteresistenz und Nachrüstbarkeit in bestehende Maschinen aus. Hersteller können auch softwarebasierte Aktivierungsdateien als Träger der Nutzungsrechte einsetzen und diesen an einen Fingerabdruck ihres Zielsystems binden.
Für einen hohen Sicherheitsgrad sorgen 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. Immer wird die zu schützende Software vollständig verschlüsselt und nur, wenn die passende Berechtigung vorliegt, der jeweils benötigte Teil entschlüsselt.

Fazit
Da Embedded-Systeme vielfältig sind, muss die Schutzlösung ebenfalls vielseitig sein. Besonders wichtig ist, dass das Schutzkonzept moderne Anforderungen der intelligenten Produktion erfüllt. Am Beispiel der Stickmaschine wird deutlich, wie Codemeter die unterschiedlichen Schutzbedürfnisse erfüllt. Hersteller können bei dessen Einsatz sicher sein, ihre Software und das Know-how darin bei der Auslieferung, im Betrieb, bei der Aktualisierung der Firmware oder der Freischaltung neu erworbener Funktionen zu schützen. Nicht zuletzt dank dieser Eigenschaften hat es Codemeter zu einem von rund 200 Beispielen auf der Industrie-4.0-Praxis auf die deutschlandweite Online-Landkarte der Plattform Industrie 4.0 geschafft. (ih)

Oliver Winzenried ist Vorstand und Mitgründer der Wibu-Systems AG in Karlsruhe. info@wibu.com