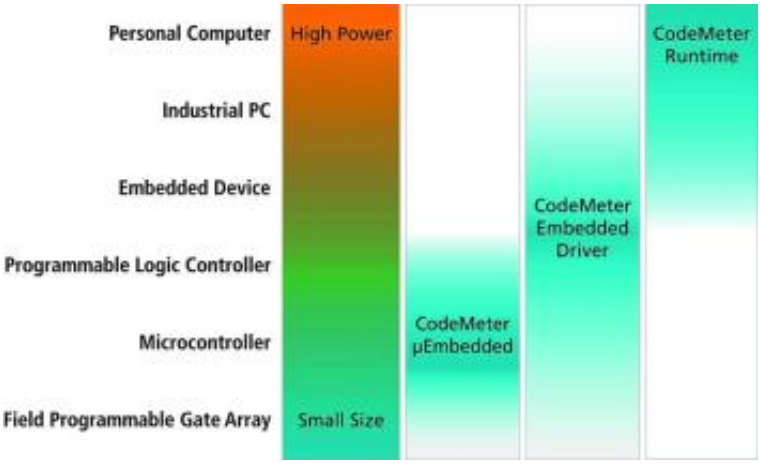
wirautomatisierer.de

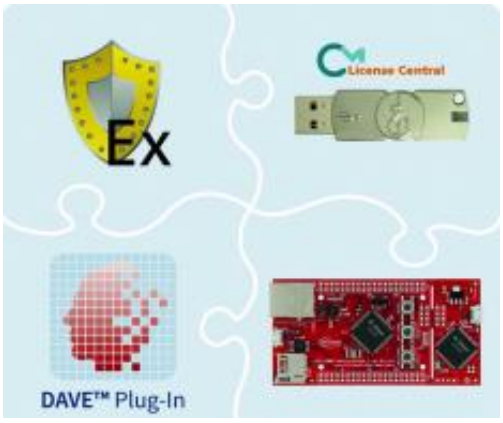


In der intelligenten Produktion von heute werden Geräte, Maschinen und Anlagen vernetzt, sodass sie miteinander kommunizieren können: Sie verarbeiten Daten und Signale, steuern, regeln und überwachen. Grundlage dafür ist die Embedded-Software, die viel Know-how enthält, für das sich auch Wirtschaftsspione, Produktpiraten oder Cyber-Angreifer interessieren. Die Hersteller haben jedoch erkannt, dass die Faktoren Schutz, Integrität und Lizenzierung für den Geschäftserfolg wichtiger werden.

CodeMeter schützt und lizenziert auf ganz unterschiedlichen Plattformen Bild: Wibu-Systems

Wie Hersteller ihre Embedded-Soft- und Firmware schützen können

Schutz und Integrität als Erfolgsfaktoren



CodeMeter-Plug-In für Dave Bild: Wibu-Systems

Unterschiedliche Bauformen der CodeMeter-Schutzhardware und der softwarebasierten Lösung Bild: Wibu-Systems

Am Beispiel der von Wibu-Systems entwickelten CodeMeter-Technologie, einer technisch-präventiven Lösung, können Hersteller klassische PC-Software aber auch Embedded-Software ihr Know-how wirkungsvoll vor Hackern, Produktpiraten und Saboteuren schützen oder ihre Software lizenzieren. Gleichzeitig erfüllt CodeMeter die unterschiedlichen Sicherheitsbedürfnisse der Industrie, einschließlich moderner Security für Industrie 4.0 und das Internet der Dinge. Dabei wird die Embedded-Software ver- und entschlüsselt, die notwendigen Schlüssel sicher gespeichert und der Programmcode vor Manipulation durch elektronisch signierten Code und die Prüfung gegen eine Zertifikatskette geschützt. Je nach Größe und Leistungsfähigkeit der Plattform kommen neben CodeMeter Runtime auch CodeMeter Embedded oder CodeMeter µEmbedded zum Einsatz.

CodeMeter Embedded

Als schlanke Variante der CodeMeter Runtime können Hersteller CodeMeter Embedded für Embedded-Systeme wie Windows Embedded, Linux Embedded, VxWorks, QNX oder SPSen nutzen. Der Hersteller verschlüsselt und signiert seine Embedded-Software und liefert sie als geschützte Version auf einem Gerät, einer Maschine oder einer Anlage an den Anwender aus. Nur mit der vom Hersteller gelieferten, passenden Schutzhardware CmDongle oder der passenden Aktivierungsdatei CmActLicense kann der Anwender die geschützte Software nutzen. Dazu wird der jeweils zur Laufzeit benötigte Teil der Software geprüft und entschlüsselt.

Entweder können Hersteller Verschlüsselungsfunktionen der CodeMeter-API selbst in ihre Embedded-Software einbauen oder mit dem Tool AxProtector for CmE arbeiten. Der AxProtector for CmE schützt die Software automatisch und sicher ohne Änderungen am Quellcode. Er ist als grafische Oberfläche verfügbar oder kann per

Kommandozeilenwerkzeug als Post-Build-Prozess in ein automatisches Build-System integriert werden.

CodeMeter µEmbedded

Für Embedded-Systeme mit noch geringerem Speicherplatz gibt es CodeMeter µEmbedded. Die Lösung enthält den minimal notwendigen Funktionsumfang und hat nur einen geringen Speicherplatzbedarf: 60 Kilobyte für die Schutzfunktionen oder etwa 80 Kilobyte, wenn Module der Embedded-Software lizenziert werden sollen. Die eindeutige ID des Logikbausteins oder des Mikrocontrollers dient als Anker für die Lizenzen, die daran gebunden werden. Danach werden die Lizenzen für die Produktion aktiviert. Sie sind mit allen CodeMeter-Varianten kompatibel. Sobald der Anwender weitere Funktionen nachträglich erwirbt, kann der Hersteller diese per Dateiaustausch freischalten.

CodeMeter µEmbedded legt darüber hinaus symmetrische und asymmetrische Schlüssel in einem geschützten Speicherbereich ab, der nur von Geräten mit passender ID nutzbar ist. Typische Anwendungsfälle sind Lizenzkontrolle von Geräten, Überwachung von Produktionsmengen durch Lizenzierung der einzelnen hergestellten Geräte sowie die sichere, verschlüsselte Übertragung von Programmcode und Updates in ein Gerät.

Bestandteil der Infineon-Entwicklungsumgebung

Hersteller, die mit der Eclipse-basierten Entwicklungsumgebung Dave 4 von Infineon ihre Software entwickeln, können ab sofort das kostenfreie CodeMeter Plug-In, das in Dave 4 integriert wurde, für eigene Anwendungen nutzen. Dave generiert den passenden Code für die XMC-Mikrocontroller; der Anwender kann vorhandene kommerzielle Third-Party-Tools für ARM nutzen, linken und auf den Mikrocontroller laden. Das Plug-In enthält die CodeMeter-µEmbedded-Technologie von Wibu-Systems, darunter den ExProtector, sodass der Entwickler Programmcode verschlüsselt und signiert. Eine einfache, grafische Oberfläche im neuen Plug-In konfiguriert XMC4000-Mikrocontroller und erzeugt verschlüsselte Firmware-Updates oder Lizenzen.

Schutz von Firmware und sichere Firmware-Updates

Ein Gerätehersteller entwickelt ein neues Gerät und bringt es auf den Markt. Zu Beginn wird aus Dave heraus eine Firmware v1.0 erzeugt, die am Ende mit Hilfe des neuen Plug-Ins und des ExProtectors automatisch verschlüsselt wird. Vor der Auslieferung wird der XMC4000-Mikrocontroller in der sicheren Umgebung des Geräteherstellers mit einem mitgelieferten, sicheren Bootloader ausgestattet, der schreibgeschützt im Controller gespeichert wird. Dann wird ein an die ID dieses Controllers gebundener Lizenzcontainer erstellt und schließlich die verschlüsselte Firmware v1.0 auf das Gerät geladen. Mit Hilfe eines automatisierten Programmierprozesses können die Geräte schnell programmiert werden; der Vorgang läuft technisch ähnlich ab wie ein herkömmlicher Firmware-Downloadprozess in der Serienfertigung.

Die neue Firmware v2.0 wird über Dave erzeugt, getestet und dann mit dem ExProtector automatisch signiert und verschlüsselt. Danach ist die Firmware gesichert und kann zum Kunden geschickt und dort aufgespielt werden, ohne dass Angreifer sie beim Transport oder beim Kunden mitlesen oder ändern können. Der Ladeprozess beim Kunden entschlüsselt die Firmware im Mikrocontroller, legt sie in dessen Speicher ab und prüft die Signatur. Ist diese korrekt, kann das Gerät starten, anderenfalls wird der Start abgebrochen.

Wurde das Gerät mit einer universellen Firmware ausgestattet, kann der Hersteller zusätzliche Funktionen nachträglich freigeschalten. Das separate CodeMeter-Tool License Central speichert beim ersten Programmieren die ID des Controllers. Mit der Seriennummer seines Controllers kann ein Kunde über ein Lizenzportal des Herstellers weitere Funktionen in Form einer neuen Lizenzdatei erwerben. Die neue Lizenzdatei passt nur zu diesem Controller; ein Austausch der Firmware ist nicht nötig. ge

KONTAKT

Wibu-Systems AG

Karlsruhe

Tel. 0721 93172-0

www.wibu.com

Hannover Messe: Halle 8, Stand D05

Weitere Informationen zum Thema:

http://t1p.de/9nzx

Der Autor: Dipl.-Ing. Oliver Winzenried, Vorstand der Wibu-Systems AG und Vorsitzender der VDMA-Arbeitsgemeinschaft Produkt- und Know-how-Schutz

17.03.2016