

Sichere Hardware soll Software vor Produktpiraten schützen

Mit aktueller Technik gegen die Produktpiraterie

Zu den Themen, die auf der Hannover-Messe die größte Aufmerksamkeit genießen, gehören die Produktpiraterie und der Schutz davor. Die Karlsruher Firma Wibu-Systems entwickelt schon seit langem Produkte, die den Diebstahl von Software-IP (Intellectual Property) verhindern sollen. Oliver Winzenried, CEO von Wibu-Systems, informiert darüber, welche Gefahren bestehen und was die betroffenen Unternehmen dagegen tun können.

Markt&Technik: Als wie stark betrachten Sie die Bedrohung vor allem aus China bzw. Fernost für die Software von Maschinen und Anlagen hierzulande?

Oliver Winzenried: Unser Firmenslogan »Perfection in Software, Document, Media and Access Protection« beschreibt, was wir tun, nämlich Schutz und Lizenzierung digitaler Produkte, und wie wir es tun: möglichst perfekt, also mit einem hohen Schutzgrad.

Nach der »BSA/IDC-Global-Software-Piracy«-Studie* sind im weltweiten Durchschnitt 35 Prozent der genutzten Software nicht lizenziert und bezahlt und werden somit als »Raubkopie« genutzt. Laut einer VDMA-Umfrage,

deren Ergebnisse im April 2008 vorgestellt wurden, sind 52 Prozent der Maschinen- und Anlagenbauer vom Nachbau kompletter Maschinen betroffen. Die Bedrohung durch Software-Piraterie aus Fernost ist prozentual stärker als im weltweiten Durchschnitt, allerdings ist der absolute Schaden auf der Software-Seite in den etablierten Märkten noch höher, weil hier weit mehr Software im Einsatz ist. Gerade im Maschinen- und Anlagenbau ist das Risiko groß, durch Software-Piraterie den Know-how-Vorsprung einzubüßen. In Maschinen wird, wie beispielsweise auch im Automobil, ein immer größerer Teil des Funktionsumfangs in Software realisiert.

Welche Techniken und Schutzmaßnahmen sollten deutsche bzw. europäische Automatisierungstechnik-Hersteller nutzen, um den Schutz ihrer IP sicherzustellen?

Automatisierungstechnik-Hersteller sollten verschiedene Schutzmaßnahmen ergreifen: Rechtliche Maßnahmen wie etwa Patente, Geschmacksmuster und Warenzeichen, aber auch Kennzeichnungsverfahren und – besonders wichtig – konstruktive Maßnahmen, die präventiv das Kopieren und Nachbauen erschweren. Gerade für IP, also Pläne, Serviceunterlagen, Produktionsdaten und Software, gibt es Verfahren, die die digitalen Produkte durch harte Verschlüsselung schützen und den Schlüssel oder die Nutzungslizenzen in einer sicheren, nicht manipulier- und nachbaubaren Hardware speichern. »CodeMeter« von Wibu-Systems ist eine bewährte Lösung für Desktop-PCs, die im Rahmen des Projekts »Pro-Protect« gemäß den Anforderungen der Industrie erweitert wird.



Oliver Winzenried, Wibu-Systems

» Konstruktive Maßnahmen, die präventiv das Kopieren und Nachbauen erschweren, schützen am besten vor unerlaubter Nachahmung. «

Ein wichtiger Punkt ist der Schutz von Embedded-Software. Welche Möglichkeiten gibt es, sie zu schützen?

Embedded-Software lässt sich mit denjenigen Verfahren schützen und lizenzieren, die sich auch für Desktop-PCs eignen: Verschlüsselung von Programm-Code und Ressourcen, Obfuskierung (Verschleierung von Programm-Code), Anti-Debugging-Mechanismen sowie Authentifizierung. Die Nutzung von Schutz- und Lizenzierungsverfahren bringt zusätzliche Vorteile wie etwa Versionskontrolle. Zudem stellt sie sicher, dass nur passende Software-Versionen gleichzeitig genutzt werden, und ermöglicht die Nutzungsmessung. Die Logistik der Verteilung lässt sich vereinfachen.

Ein Problem im Software-Segment sind »juristische Grauzonen« innerhalb Europas. Wie können betroffene Unternehmen dem begegnen?

Die Grauzone betrifft die Patentierbarkeit computer-implementierter



CompactFlash-Karte schützt Software und Produktionsdaten vor Diebstahl

Erste CompactFlash-Karte mit »CodeMeter«-Technik

Auf der Hannover-Messe stellt Wibu-Systems den Prototypen einer CompactFlash-Karte vor, die auf der Kopierschutztechnik »CodeMeter« des Unternehmens beruht. Gedacht ist die als »CmCF Card« bezeichnete CompactFlash-Karte für den Maschinen- und Anlagenbau. »Den bestmöglichen Schutz vor Produktpiraterie und Industriespionage bieten Hardware-gestützte Systeme«, erläutert Oliver Winzenried, Gründer und CEO von Wibu-Systems. »Wir bieten solche Systeme für die verschiedensten Plattformen und Schnittstellen an – ab der zweiten Jahreshälfte und als Beitrag zur Initiative »Pro-Protect« auch für die CompactFlash-Schnittstelle, die im Maschinen- und Anlagenbau weit verbreitet ist.«

Aus Sicht von Maschinen- und Anlagenbauern müssen Lösungen zum Schutz vor Produktpiraterie

folgende Anforderungen erfüllen: Sicherheit, Nachrüstbarkeit, Flexibilität und Robustheit im Fabrik-Alltag. »Unsere »CmCF Card« erfüllt diese Anforderungen: Sie ist sicher wie jede Schutztechnik auf »CodeMeter«-Basis und flexibel einsetzbar in SPS-Systemen sowie unter Windows CE, Real-time-Linux und weiteren Echtzeitsystemen«, verdeutlicht Winzenried. »Bei Temperaturen von -25 bis +85 °C funktioniert sie zuverlässig, und im Inneren der Maschine ist sie geschützt vor Staub, Feuchtigkeit und starken elektrischen und magnetischen Feldern. Zudem ist sie nachrüstbar und lässt sich daher in bereits bestehende Maschinen und Anlagen integrieren.«

Auf der Hannover-Messe können sich interessierte Unternehmen am Gemeinschaftsstand »Plagiat-



In Maschinen und Anlagen schützt die »CmCF Card« von Wibu-Systems Embedded-Software und Produktionsdaten.

schutz« (Halle 17, Stand A26) über den Prototypen der »CmCF Card« informieren. (ak)

tierter Erfindungen. Leider wurde hier in Europa noch keine echte Rechtssicherheit geschaffen. Dennoch ist bei Software eine Patentierung oft möglich, aber teuer und langwierig. Präventive technische Maßnahmen, die das Kopieren erschweren, sind daher immer zu ergreifen, unabhängig von der Patentierung.

Vor allem die juristischen und politischen Unzulänglichkeiten in China machen dieses Land zu einer Hochburg des Diebstahls von Software-Know-how. Was wünschen Sie sich von Seiten

der Politik, um die Software-Produkte europäischer Unternehmen besser zu schützen?

Ein klares und einheitliches Urheber- und Patentrecht ist sicherlich wünschenswert. In der Praxis werden Unternehmen aber immer einen Mix aus Schutzmaßnahmen benötigen, und präventive Maßnahmen spielen dabei eine wichtige Rolle, unabhängig von den Märkten.

*Das Interview führte
Andreas Knoll*

Link zur Studie: <http://www.bsa.org/germany/piraterie/upload/IDC-Impact-Study-complete-english.pdf>



Aktion »Pro-Protect« gegen Produktpiraterie

Produktionsdaten durchgängig schützen

»Pro-Protect« ist eines von zehn Projekten der Ausschreibung »Innovation gegen Produktpiraterie« des BMBF (Bundesministerium für Bildung und Forschung). Es wird von Wibu-Systems koordiniert, und das FZI (Forschungszentrum Informatik) sowie die Anwenderfirmen Homag, ZSK Stickmaschinen und GIS nehmen daran teil. Gemeinsam erarbeiten die vier Partner seit Januar 2008 Maßnahmen zum Schutz von Maschinen und Anlagen vor Produktpiraterie und Industriespionage. Im Einzelnen lauten die Ziele von »Pro-Protect«:

- Entwicklung einer nicht manipulier- und kopierbaren Schutz-Hardware für industrielle Schnittstellen und Betriebsbedingungen. Dies erschwert den Nachbau kompletter Maschinen und Anlagen durch wirkungsvollen Schutz der Embedded-Software, die einen immer größeren Anteil an Funktionsumfang und Wertschöpfung hat.

- Durchgängiger Schutz von Produktionsdaten vom Design bis zur Maschine, um unkontrollierte Produktion von Graumarkt-

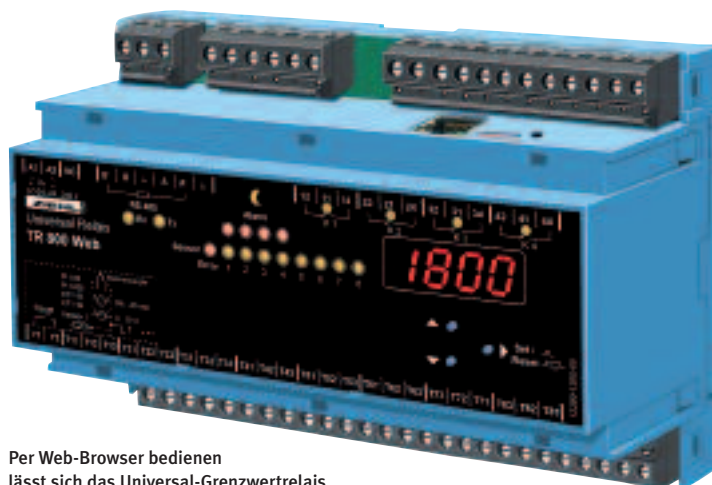
Erzeugnissen durch Fertigungszulieferer zu verhindern.

- Einführung eines »Digitalen Maschinentagebuchs« zur Effizienzsteigerung im Service und zum Schutz derjenigen Service-Dokumente, die viel Know-how enthalten.

»Die Basisanalyse hat auch bei nicht im Konsortium beteiligten Unternehmen großes Interesse an einer nachrüstbaren, sowohl von der SPS als auch von Echtzeitbetriebssystemen wie Windows CE und Realtime-Linux unterstützten Schutz-Hardware geweckt«, betont Oliver Winzenried, CEO von Wibu-Systems. Sein Unternehmen bietet bereits Lösungen für die USB-Schnittstelle und als ExpressCard sowie Prototypen der industrietauglichen »CodeMeter«-Schutz-Hardware als CompactFlash-Card und SD-Card. »CodeMeter SDL« (Secure Data Layer) ist ein Verfahren zum Schutz von Daten, und »CodeMeter License Central« ermöglicht die Erstellung, Verwaltung und Auslieferung von Lizenzen und deren Integration in Unternehmensprozesse und ERP-Systeme wie SAP. (ak)

Universal-Relais von Ziehl mit acht Analogeingängen

Web-fähiges Grenzwertrelais



Per Web-Browser bedienen lässt sich das Universal-Grenzwertrelais »TR 800 Web« von Ziehl industrie-elektronik.

Ziehl industrie-elektronik stellt auf der Hannover-Messe ein Web-fähiges Grenzwertrelais mit Ethernet-Schnittstelle und acht Eingängen für Signale von Temperatursensoren oder andere Analogsignale vor.

Das als »TR 800 Web« bezeichnete Universal-Grenzwertrelais lässt sich mit einem Intranet oder dem Internet verbinden und mit einem geeigneten Internet-Browser über TCP/IP vom PC aus bedienen und abfragen. Zur Bedienung sind keine besondere Software und keine Vorkenntnisse erforderlich. Das Relais überwacht und protokolliert gleichzeitig bis zu acht unterschiedliche Eingangssignale. Anwender können jedem der vier Ausgangsrelais bis zu acht Grenzwerte zuordnen, jeweils einen pro Eingang. Bei Über- oder Unterschreiten eines Grenzwerts löst das Relais Alarm aus: Der jeweilige Relaiskontakt schaltet um, und eine E-Mail wird abgesetzt. Bei Verlassen des Alarmzustands schaltet das Relais zurück, und ei-

ne weitere E-Mail wird, wenn gewünscht, automatisch versandt. Eine Tag/Nacht-Umschalt-Funktion erlaubt es, Grenzwerte zeitabhängig zu verändern.

Das Gerät bietet eine RS-485-Schnittstelle mit den Protokollen Modbus und Ziehl-Standard. Seine acht Messeingänge sind für folgende Signale ausgelegt (je Eingang einzeln programmierbar):

- Pt100 und Pt1000 in Zwei- oder Drei-Leiter-Technik;
- KTY 83 oder KTY 84;
- Thermoelemente Typ B, E, J, K, L, N, R, S, T;
- DC 0-10 V, DC 0/4-20 mA, Anzeige skalierbar;
- Widerstand 0-500 Ohm, 0-30 kOhm. (ak)

Halle 11, Stand D11, www.ziehl.de