

Embedded-Software und Produktionsdaten schützen Innovationen gegen Imitate



Seit 2006 geistert ein „Musterbeispiel“ für Produktpiraterie durch die Medien: Die Motorsäge MS 380 von Stihl unterscheidet sich kaum von ihrem Plagiat aus dem Unternehmen Swool im chinesischen Zhejiang. Oft hängt der Schutz der Produkt-Innovation vom Schutz der Software ab, denn der Software-Anteil an Innovationen im Maschinen- und Anlagenbau nimmt ständig zu.

Bildquelle Motorsägen: Stihl

Der Schutz vor Produktpiraterie gewinnt im Investitionsgüterbereich an Bedeutung – schlechte Erfahrungen reichen von gefälschten Ersatzteilen bis hin zu Nachbauten von komplexen Gesamtanlagen. Auf Grund des Wandels hin zur Informationsgesellschaft werden aus volkswirtschaftlicher Sicht im heutigen globalen Wettbewerb gerade für Hochlohnländer wie Deutschland Schutzmechanismen für Intellectual Property immer wichtiger, um durch eine Eindämmung der Produktpiraterie die Ertragssituation der Unternehmen zu stärken, Arbeitsplätze zu schaffen und den Innovationsvorsprung zu halten. Anders als in den Bereichen Geschäftssoftware und digitale Medien, wo sichere, hardwareunterstützte Schutzmechanismen bereits etabliert sind und in zunehmendem

Maße gegen Produktpiraterie schützen, sind effiziente Schutzverfahren im Bereich von Embedded-Software und Produktionsdaten kaum vorhanden. Aus Mangel an standardisierten Lösungen werden von den Herstellern oft aufwändige, nur zweifelhaften Schutz bietende proprietäre Lösungen umgesetzt. Ein Konsortium hat sich das Ziel gesetzt, im Desktop-Computing existierende Lösungen zum Software-Schutz auf den Bereich der Produktion zu übertragen, um den Anforderungen des Maschinen- und Anlagenbaus für durchgängigen Schutz gegen Gefahren der Produktpiraterie gerecht zu werden. Zu den Projektpartnern aus den Bereichen IT-Forschung, CAD-Software und Maschinenbau gesellt sich ein Hersteller von Digital Rights Management (DRM)-Systemen. Der Nachbau von Maschinen und

Komponenten, die mit komplexen Software-Funktionen ausgestattet sind, soll auf diese Weise erschwert werden. Auch sollen Methoden oder Verfahren abgewehrt werden, die auf das nicht autorisierte Kopieren und Nutzen aufwändiger Maschinensteuerungsprogramme zur Herstellung von geklonten Produkten abzielen.

Die Ansprüche steigen

Durch ein möglichst umfassendes Engineering-Konzept und durch den Einsatz eines offenen DRM-Systems kann ein Weg beschritten werden, der neben allen notwendigen gesetzgeberischen Maßnahmen einen eigenen Beitrag zur Eindämmung von Produktpiraterie leistet. Da der Entwicklungsaufwand für den Angreifer umso mehr

steigt, je höher die Stufe der eingesetzten Sicherheitskomponenten ist, empfiehlt es sich, bei hochwertigen Investitionsgütern auf Hardware-basierten Schutz wie Dongle oder Security Cards zu setzen, insbesondere wenn die Lizenzspeicher für mehrere Lizenzgeber nutzbar sind und dem gemeinsamen Interesse dienen, die Integrität einer Produktionskette oder Produktionsplattform zu wahren. Eine weitere Komponente im Bereich der Schutzanwendungen im Maschinenbau kann das elektronische Maschinentagebuch sein, das der Projektpartner Homag im Konortium der Initiative ProProtect als zentrale Aufgabenstellung vorsieht. Das Maschinentagebuch oder die elektronische Maschinenakte kann sehr umfangreiche und höchst schützenswerte Daten enthalten. Diese reichen bis zur Speicherung von komplexen CAD-Dateien, die alle relevanten Konstruktionsdaten von Baugruppen einer komplexen Maschine oder Anlage enthalten können. Das Vorhalten solch umfangreicher Dateien in der Maschine am Aufstellungsort bietet Vorteile für alle Arten von Servicedienstleistungen, die vom Hersteller oder von einem autorisierten Dienstleister zu erbringen sind.

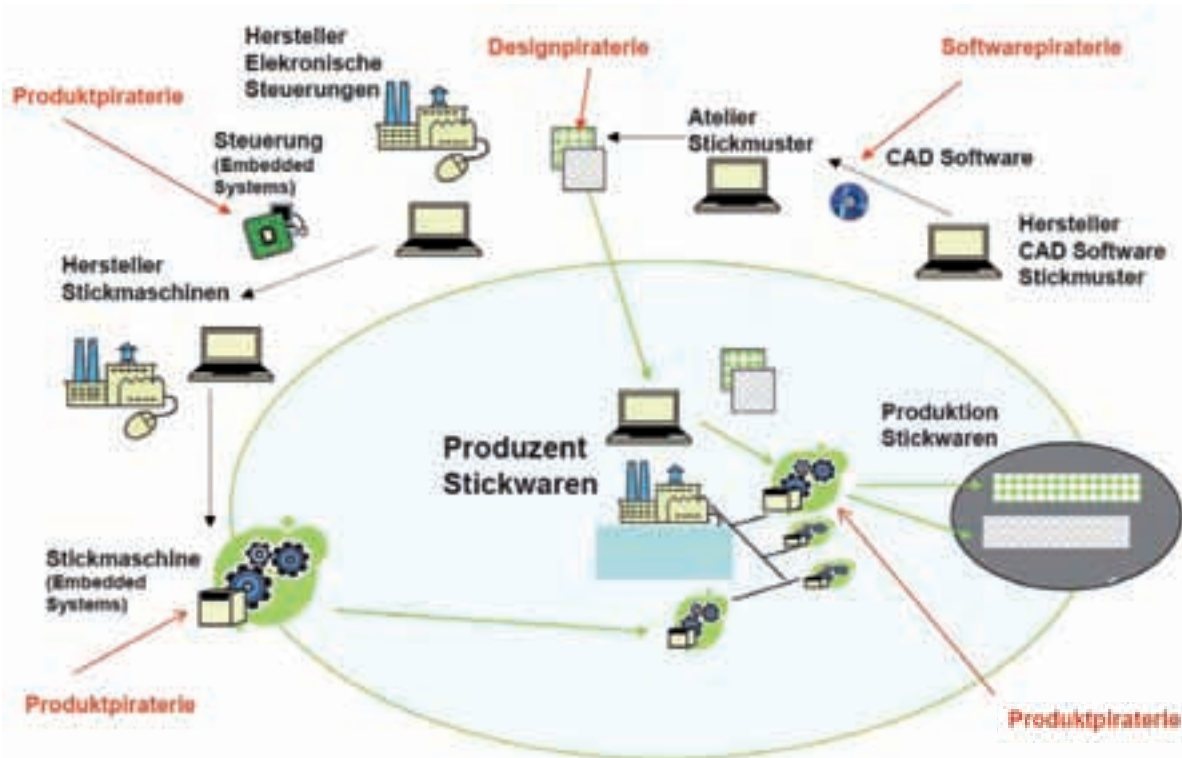
Durchgängige Schutzstrategie

Die Bedeutung von Software für den Maschinen- und Anlagenbau wird in den kommenden Jahren weiter stark zunehmen. Für den Schutz vor Produktpiraterie werden daher effiziente Software-Schutzmechanismen benötigt, die nach heutigem Stand der Technik nicht zur Verfügung stehen. Sowohl bei den produkt- als auch bei den prozessbezogenen Ansätzen besteht für die Industrie akuter Handlungsbedarf zur Herstellung und zum Ausbau des Schutzes. Erst eine gezielt auf die situationspezifischen Anforderungen ausgerichtete Wahl der Schutzstrategie und eine sorgfältige Auswahl und Kombination geeigneter Schutzansätze sowie ihre konsequente Umsetzung ermöglichen eine wirkungsvolle Abwehr von Produktpiraterie. Bisher verfügbare Technologien und Methoden bieten nur begrenzten Schutz, der in Zukunft nicht ausreichen wird. Defizite liegen dabei in allen Bereichen, da ein systematischer Schutz durch die genannten Ansatzpunkte bisher nicht realisiert werden kann. Zukünftig werden Unternehmen ihre Produkte durch übergreifende Strategien gezielt vor Piraterie schützen müssen. Dazu muss der Piraterieschutz auf die gesamte

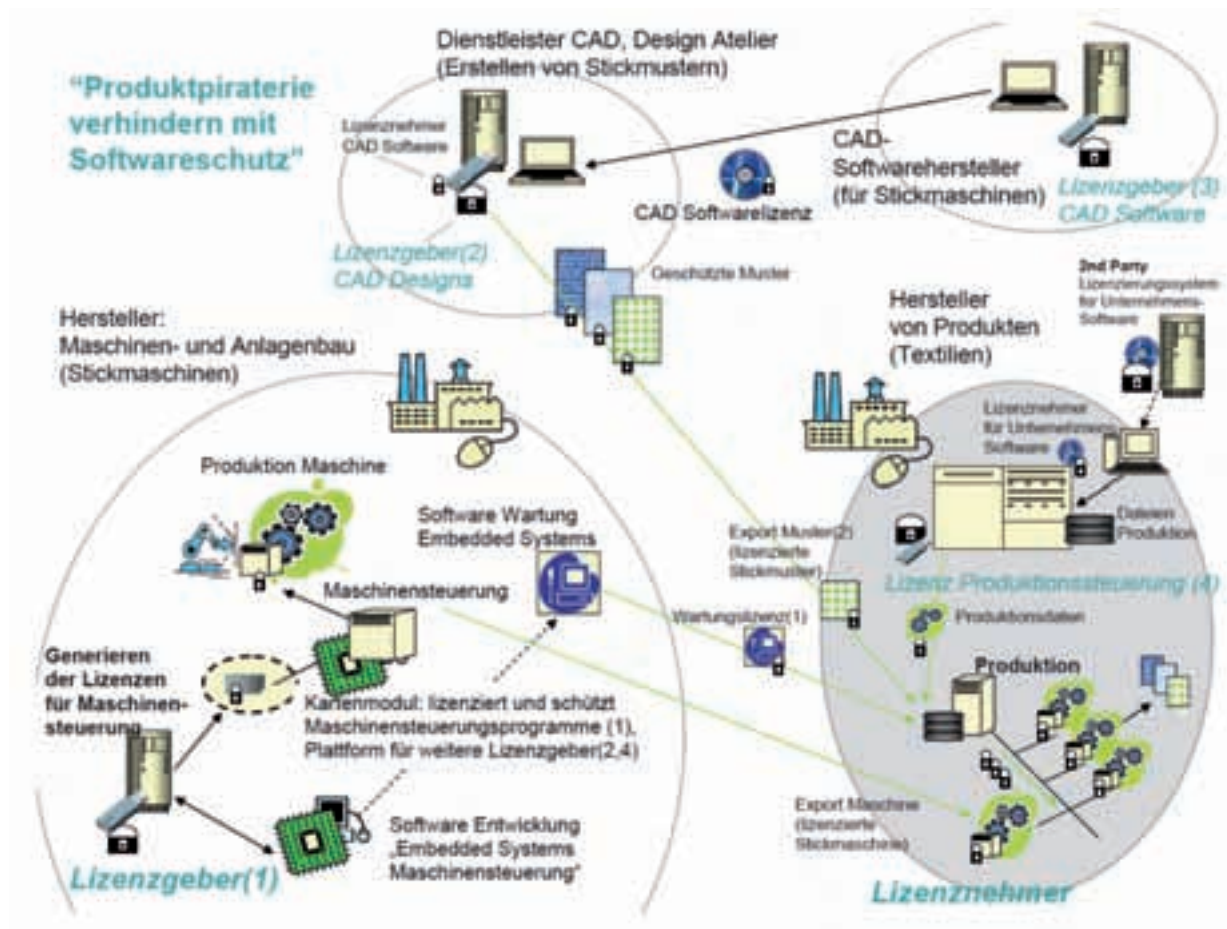
Wertschöpfungskette ausgeweitet werden. Es handelt sich also um eine gemeinsame Aufgabe aller Funktionen eines Unternehmens, die Einkauf, Entwicklung, Produktion, Rechtsabteilung, IT-Infrastruktur, Marketing, Vertrieb und After Sales sowie die gesamte logistische Kette über Zoll und Händler bis zum Kunden mit einschließt. Im Rahmen des Projekts ProProtect sollen daher umfassende Schutzkonzepte, neue Methoden sowie innovative technische Lösungen für eine durchgängige Schutzstrategie entwickelt werden, die die gesamte Wertschöpfungs- und Logistikkette konsistent von der Rohmaterial-Wertschöpfung beim Lieferanten bis zur Entsorgung beim Kunden umfasst.

Auch in kritischen Märkten

Durch eine intelligente Gestaltung und Kombination von Produkteigenschaften und Produktfunktionen, verknüpft mit einem neuartigen Informationsmanagement innerhalb und außerhalb des Unternehmens, kann Produktpiraterie weiter erschwert werden. Hierzu sollen im Rahmen des Projekts bestehende Möglichkeiten in Schutzstrategien systematisiert und in ihrer Wirkung bewertet werden. Wirkungsvolle, neue Instru-



Ein Beispielszenario: Die Abbildung zeigt, an welchen Stellen Produktpiraterie in der Produktionskette zur Gefahr für geistiges Eigentum werden kann. Im Szenario wird der Hersteller von Stickmaschinen betrachtet, der seine Maschinen an einen Produzenten von Textilien liefert, dessen Produktionsstandort sich an einem beliebigen Punkt der Erde befinden kann.



Das dargestellte Szenario zeigt den Einsatz einer steckbaren Hardwareschutzkomponente, um Produkte und Komponenten, die auf hoch entwickelten Technologien basieren, vor Angriffen durch Produktpiraterie zu schützen. An erster Stelle stehen die Maßnahmen, die den Schutz von Software vorsehen, aber auch der Schutz von Daten ist Bestandteil eines erweiterten Schutzkonzeptes.

mente werden erforscht, die Neu- und Weiterentwicklung von Schutzmethoden und -technologien sowie integrierten Ansätze sollen vorangetrieben werden, um einen effizienten und effektiven Schutz vor Produktpiraterie zu gewährleisten. So wird eine Lösung entstehen, die es Anwendern im Maschinen- und Anlagenbau ermöglicht, ihre überwiegend in Software-Komponenten realisierten Innovationen sowie anderes geistiges Eigentum, zum Beispiel Lizenz- und Urheberrechte in Produktionsdaten, auch in kritischen Märkten vor Produktpiraterie und Lizenzverstößen zu sichern. Dieser Ansatz wird von den beteiligten Anwendungspartnern in verschiedenen Anwendungsszenarien (Stickmaschinen und Stickmustererzeugung, Holzbearbeitungsmaschinen und zugehörige Fertigungsdaten) über Pilotvorhaben während der Projektlaufzeit evaluiert. Eine Übertragung in andere Anwendungsbereiche ist durch den offenen Ansatz problemlos möglich.

Stand der Dinge

Auch wenn die zunehmende Bedrohung durch Produktpiraterie im Maschinen- und Anlagenbau seit einigen Jahren verstärkt wahrgenommen wird, sind bislang nur wenige allgemeine und herstellerübergreifende Maßnahmen zum Schutz der Produkte bekannt. Maßnahmen zur Kennzeichnung der Produkte, zum Beispiel durch Hologramm oder RFID-Etiketten, wie zum Teil auf Software-Verpackungen genutzt, stellen keinen effizienten Schutz dar, da sich die Endnutzer im Allgemeinen der Lizenzverstöße bewusst sind oder das Piraterieprodukt sogar selbst herstellen. Im Bereich eingebetteter Hard- und Software greifen einige Hersteller zu eigenentwickelten Lösungen wie Software-Aktivierungen durch Lizenzschlüssel, Verschlüsselung von Daten mit eigenen Algorithmen und, zum Beispiel im Bereich der Automobilhersteller, auch gegenseitige Authentifizierung von

vernetzten Steuergeräten. Doch leider sind auch diese Schutzmaßnahmen erwiesenermaßen unzureichend:

- Aufgrund fehlender Hardware-Unterstützung (zum Beispiel „tamper-resistent“ Hardware) sind die Mechanismen meist mit geringem Aufwand mittels „Klonen“ zu umgehen.
- Einfache eigenentwickelte Lösungen ermöglichen kein komplexes Lizenzmanagement, das für flexible Vertriebs- und Vergütungsformen nötig ist, und verfügen auch über keine Anbindung an externe Lizenz- oder Warenwirtschaftssysteme.
- Schutzmaßnahmen werden speziell für bestimmte Geräte oder Anlagen entwickelt und sind nicht auf andere Hard- oder Software-Plattformen übertragbar, wodurch sich ein unverhältnismäßig hoher Aufwand für die Entwicklung ergibt.

Eine Hardware-unterstützte, generische Lösung für das Lizenzmanagement von Embedded-Systemen kann Abhilfe schaffen.

Solche Lösungen sind aber bisher nur für PC-Plattformen verfügbar. Hier existieren komplexe Lizenzmanagementsysteme wie das CodeMeter-System des Verbundpartners Wibu, die eine einfache Integration in Software-Produkte und einen flexiblen, sicheren (Hardware-basierten) Schutz zu geringen Kosten ermöglichen. Ebenso existieren etablierte DRM-Lösungen, die einen einfachen Lizenzschutz von digitalen Daten und Medien ermöglichen. Diese nutzt zum Beispiel die Musikindustrie. Auf den Embedded-Bereich lassen sich die Lösungen jedoch nicht übertragen: Embedded-(Echtzeit)-Betriebssysteme und -Hardware-Schnittstellen werden nicht unterstützt und eine Integration in den Entwicklungsprozess steht nicht zur Verfügung. So ist das Lizenzmanagement für Software heute meist als mehr oder weniger sorgfältig durchgeführte Aufgabe in Verantwortung des Anwenders zu sehen.

Proprietär – Eine Lösung?

Produzierenden Industrieunternehmen fehlt eine systematische Vorgehensweise, um die eigenen Produkte wirkungsvoll gegen die zunehmende Produktpiraterie zu schützen. Der Stand der Technik im Produktschutz basiert vielfach auf eigenentwickelten Verfahren, wobei zumeist eine programmierbare Identitätsnummer für eine elektronische Steuerung (oder eine programmierbare und auslesbare Maschinen-Identnummer) Anwendung findet. Spezielle, einmal programmierbare Speicher enthalten den Seriencode, der mit den Komponenten der elektronischen Steuerung elektrisch verbunden ist. Der Schutz vor dem Auslesen eines solchermaßen gespeicherten Identcodes ist mit relativ geringem Aufwand für einen versierten Angreifer zu erkennen oder zu umgehen, denn er kann gegebenenfalls durch einen Ersatzspeicher geklont werden und damit zum Einstieg für den Nachbau von elektronischen Steuerungen oder anderen Maschinenkomponenten genutzt werden. In jedem Fall sind proprietäre Schutzlösungen wenn sie auch noch mit Teilen von Steuerungsprogrammen oder Betriebssystemkomponenten logisch eng verknüpft werden, meistens schwierig zu warten und mit modular aufgebauten Komponenten- und Systemlösungen schwer in Einklang zu bringen.

Maßnahmen systematisieren

Eine Erweiterung des Schutzes auf höhere Schutzlevel ist mit viel Aufwand verbunden, da leistungsfähige Tools zur Integration der

Schutzlösungen auf Zielplattformen nicht vorhanden sind. Das zunehmende Angriffspotential, das auf den internationalen Märkten mittlerweile anzutreffen ist, lässt die Entwicklung effizienter Schutzsysteme auf der Basis proprietärer Konzepte kaum noch zu. Bisher sind noch keine Standardlösungen beziehungsweise Plattformen am Markt verfügbar, die die nötige Akzeptanz für den breiten Einsatz effizienter Schutzkonzepte zum Schutz von Maschinen und Anlagen sowie der dort zur Verarbeitung kommenden Produktionsdaten bieten. Die aktuell in der Praxis vorzufindenden Strategien beschränken sich auf die punktuelle Vermeidung der Preisgabe von Technologiewissen. Aufgrund globaler Absatzmärkte und damit notwendiger weltweiter Produktionsinfrastrukturen sind unsystematische, einfache Vermeidungsstrategien auf Dauer nicht ausreichend. Ein essentieller Faktor im Schutz vor Produktpiraterie wird sein, unterschiedliche Schutzmaßnahmen zu systematisieren, umfassend zu kombinieren und weiterzuentwickeln. Hierzu müssen geeignete branchenspezifische Strategien, Leitfäden, Methoden und Verfahren ähnlich der bekannten Systematik von Produktionssystemen entwickelt werden, um Wertschöpfungsprozesse vor unerwünschtem Know-how-Transfer zu schützen.

Juristerei gegen Technologie

Nach einer Studie des Fraunhofer-Instituts für Produktionsanlagen und Konstruktionstechnik (IPK) wurden inzwischen bereits zwei Drittel aller Unternehmen aus verschiedenen Branchen Opfer von Marken- und Produktpiraterie. Folgerichtig ist die Problematik der Marken- und Produktpiraterie für einen Großteil der Unternehmen von strategischer Wichtigkeit. Der Einsatz von Ressourcen zur Bekämpfung von Marken- und Produktpiraterie ist jedoch eher reaktiv ausgelegt. In vielen Unternehmen fehlt es an vordefinierten und etablierten Prozessen zur Bekämpfung von auftretender Piraterie. Der Grad der Improvisation ist hoch. Um gegen Produkt- und Markenpiraterie vorzugehen, greifen Unternehmen heute insbesondere auf die Strategie zurück, juristisch gegen Produktpiraterie vorzugehen. Den technologischen Schutzinstrumenten wird in der Zukunft das größte Lösungspotential vorausgesagt. (sph) ■

Dieser Beitrag entstand auf Basis des Rahmenplans zum Projekt „Produktpiraterie verhindern mit Software-Schutz“.

www.pro-protect.de

Produktpiraterie verhindern mit Software-Schutz

Das Projekt ProProtect wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Als externer Partner unterstützt der Verband Bitkom alle Aktivitäten des Konsortiums. Über den Industriearbeitskreis unterstützt der Verband die Verbreitung und Standardisierung der Ergebnisse aus dem Forschungsvorhaben. Dritte können so künftig durch den Einsatz der realisierten Standardlösungen in ähnlicher Weise profitieren wie die Anwender im Projekt. Dabei profitieren Hersteller und Anbieter von Software, Content und Medien genauso wie Anlagen- und Maschinenbauer, die ihre Maschinen und die hergestellten Produkte vor Nachbau schützen müssen.

Projektpartner

Wibu-Systems AG
 FZI Forschungszentrum Informatik
 ZSK Stickmaschinen GmbH
 GiS Gesellschaft für Informatik und Steuerungstechnik mbH
 Homag Holzbearbeitungssysteme AG

Industriearbeitskreis

Um frühzeitig potentielle Anwender in das Projekt einzubinden und deren Anforderungen in das Projekt einfließen zu lassen, wird ein Industriearbeitskreis gebildet, der neben den beteiligten Anwendungspartnern auch anderen interessierten Unternehmen offen steht. Im Rahmen des Arbeitskreises werden auch nicht direkt am Projekt beteiligten Unternehmen die erarbeiteten Ergebnisse verfügbar gemacht. Ihre Erfahrungen und Wünsche können so in die Entwicklung eingebracht werden. Die teilnehmenden Unternehmen ziehen unter anderem als Testanwender für die entwickelten Techniken und Methoden und durch Lieferung entsprechender Szenarien Nutzen aus dem Projekt.

