Standardisierte Lösungen

Industriestandards haben Auswirkungen auf die Weiterentwicklung hochvernetzter Komponenten. Standardisierte Lösungen wie CodeMeter oder TPMs reduzieren die Kosten. Betriebssysteme wie Realtime-Linux oder Windows CE und Steuerungen auf Standardplattformen ermöglichen eine einfache Vernetzung von Steuerungen und Komponenten.

Das „Internet der Dinge“ ist die logische Konsequenz aus dem Einzug der Micro PCs mit leistungsfähigen Entwicklungstools für Software in den Maschinen- und Anlagenbau.

- **Betriebssystem-Unterstützung**: Windows Embedded, Windows CE, Real-time Linux-Varianten und Echtzeit-Betriebssysteme wie VxWorks.
- **Nachrüstbarkeit**: Die Schutzlösung muss in bestehenden Lösungen verwendbar sein.
- **Höchste Zuverlässigkeit**: Höhere Anforderungen an Lebensdauer-Überwachung und Temperaturbereich sowie eine feste Stückliste der Schutz-Hardware und keine unbemerkten Firmware-Änderungen sind zwingend.

Kontakt
www.pro-protect.de

Ansprechpartner
WIBU-SYSTEMS AG
Oliver Winzenried
Wolfgang Neifer
Tel.: +49 721 93172 0
Email: pro-protect@wibu.de

Das Konsortium

FZI Forschungszentrum Informatik, Karlsruhe
Dr. Philipp Graf
www.fzi.de

GiS Gesellschaft für Informatik und Steuerungstechnik mbH
Dipl.-Inf.(FH) Heiner Schäfer
www.gis-net.de

Homag Holzbearbeitungssysteme AG
Dipl-Ing. Ulrich Doll
www.homag.de

WIBU-SYSTEMS AG
Oliver Winzenried
Wolfgang Neifer
www.wibu.de

ZSK Stickmaschinen GmbH
Michael Metzler
www.zsk.de

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

BETREUT VOM
PTKA Projektträger Karlsruhe
im Karlsruher Institut für Technologie

BITKOM VDMA ConImit Contra Imitatio

Das Ziel von Pro-Protect ist es, mit standardisierten Lösungen die Produktpiraterie bei Maschinen und Anlagen zu reduzieren.

Pro-Protect

Produktpiraterie verhindern mit Softwareschutz

FZI GiS HOMAG WIBU SYSTEMS ZSK

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

FKZ: 02PU1130

Schutz vor Produktpiraterie

Der Maschinen und Anlagenbau hat sich zunehmend mit Produktfälschungen auseinanderzusetzen. Die Spannweite reicht dabei von Ersatzteilen und komplexen Anlagen bis zur Embedded Software.

Weil der Software-Anteil an Innovationen im Maschinen- und Anlagenbau stetig zunimmt, ist ein wirkungsvoller Softwareschutz gleichbedeutend auch mit Innovationsschutz.

Geleichzeitig steigt mit zunehmender Digitalisierung der Produktion die Bedeutung des Schutzes von Produktionsdaten.

Das Ziel von Pro-Protect

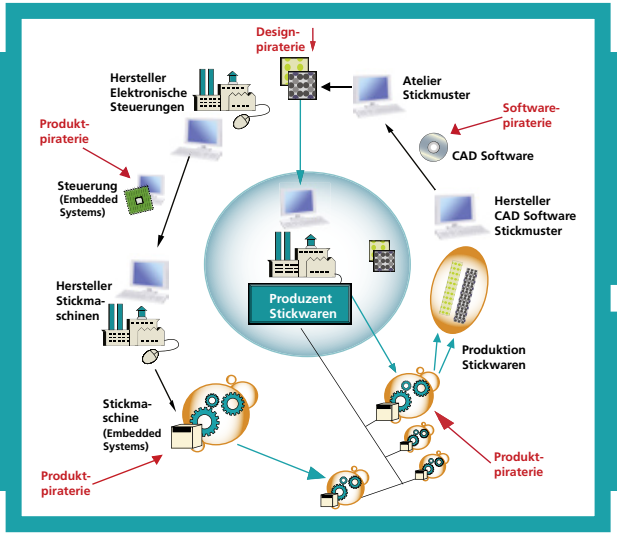
Im Fokus steht das Übertragen existierender Softwareschtuz-Lösungen auf den Bereich der Produktion:

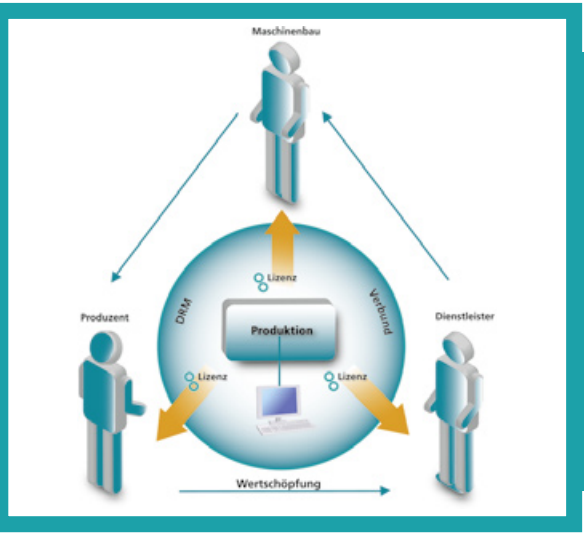
- Entwicklung einer nicht manipulier- und kopierbaren Schutzhardware zum Einbau in Maschinen. Dies erschwert den Nachbau von Maschinen sowie Komponenten, die komplexe Software-Funktionen enthalten.
- Schutz von Produktionsdaten und Prävention gegen Graumarktprodukte durch Fertigungszulieferer.
- Einführung eines „Digitalen Maschinentagebuchs“ zur Effizienzsteigerung im Service.

Nutzen für alle

Die Vision ist, mit einem offenen Schutzsystem den Nutzen für alle in der Wertschöpfungskette beteiligten Akteure zu sichern.

- **Maschinen- und Anlagenhersteller** erschweren den Maschinennachbau und generieren Mehrwert mit ihren Maschinen, die geschützte Produktionsdaten verarbeiten.
- **Schutzsystem-Hersteller** erweitern ihren Markt um Kunden aus dem Maschinen- und Anlagenbau.
- **Entwickler** verfügen über ein standardisiertes Schutzsystem mit hoher Sicherheit.
- **Dienstleister** erstellen geschützte Produktionsdaten oder beraten bei der Integration von Schutzlösungen.





Kette von Produktpiraterie

Das Bild zeigt die Kette der Produktpiraterie, angefangen bei der CAD-Software auf dem PC, über die schützenswerten Produktionsdaten, deren Nutzung kontrolliert erfolgen soll, bis zur Embedded Software, deren Schutz den Nachbau der Maschine erschwert und neue Vertriebsformen und Geschäftsmodelle ermöglicht (Pay-per-use, Leasing, etc.).

PRO PROTECT

„Harter“ Kopierschutz

SmartCard-Technologien als Bestandteil einer steckbaren Karte, eines Dongles oder eines TPM erlauben die Einbettung in die unterschiedlichsten Hardwaresysteme und Betriebssystemplattformen. Standardisierte Schnittstellen und Netzwerkfähigkeit aller Schutzkomponenten gewährleisten die Integrationsfähigkeit auch in komplexe Systemumgebungen.