

Toni Schneider

# Kopierern das Handwerk legen

Illegales Kopieren der Applikationssoftware entwickelt sich zu einem Problem im Maschinenbau. Dongle-Konzepte ähnlich denen, wie sie im PC-Umfeld bereits seit langem im Einsatz sind, bieten hier wirksamen Schutz.

Die Verwendung von Industrie-Standards bei Steuerungskomponenten bietet dem Maschinenhersteller ohne Frage zahlreiche Vorteile: Standard-Hardware- und -Software ist in zahlreichen Anwendungen erprobt und kann dank der Verbreitung in hohen Stückzahlen oft kostengünstig angeboten werden. Zudem sind die Komponenten weltweit verfügbar. Das gilt für komplette Steuerungseinheiten ebenso wie für Kommunikationssysteme und Bediengeräte.

In Bezug auf den Technologieschutz beziehungsweise die Anfälligkeit für illegales Kopieren von maschinenspezifischem Know-how, tritt allerdings ein Nachteil zu Tage, der zunehmend an Gewicht gewinnt: Je höher die Standardisierung und die weltweite Verfügbarkeit der vom Hersteller gewählten Maschinensteuerung ist, umso niedriger ist auch die Hemmschwelle, eine 1:1-Kopie anzufertigen. Das hat unterschiedliche Gründe:

- ▷ Die verwendete Hardware kann problemlos beschafft werden.
- ▷ Die Software lässt sich ohne weiteres aus einer Maschinensteuerung downloaden und in eine „leere“ Maschinensteuerung aufspielen.
- ▷ Insbesondere wenn Maschinensteuerungen mit modernen steckbaren Flashspeichern ausgestattet sind, gelingt das Kopieren der Applikationssoftware mittels beliebigen Card-Readern mit Leichtigkeit.

## Arbeitskreis „Innovationsschutz“ im VDMA

Viele Hersteller von Geräten, Maschinen oder Anlagenkomponenten haben bereits leidvolle Erfahrungen mit Kopien und Nachbauten ihrer Maschinen machen müssen. Vor allem der asiatische Raum entwickelt sich zu einem florierenden Markt von kopierten Maschinenlösungen.

Innerhalb des VDMA beschäftigen sich bereits seit geraumer Zeit Automatisierungsanbieter und Maschinenbauer mit dieser Problematik. Im Sommer 2004 wurde dort der Arbeitskreis „Innovationsschutz“ ins Leben gerufen, in dessen Rahmen Automatisierungsanbieter und -anbieter Lösungen erarbeiten, die das Kopieren von Produkten und Maschinen verhindern oder Plagiate für den Anwender leichter erkennbar machen sollen. Hierzu zählen chemische Gehäusebehandlungen, Hologramme, RFID-Technologie sowie andere elektronisch abtastbare Kennzeichnungen und insbesondere auch steuerungstechnische Maßnahmen zum Kopierschutz.

## Relativ einfach – das Einbrennen von Vendor-IDs

Eine relativ leicht zu realisierende Lösung stellt das Einbrennen so genannter Vendor-IDs in „einmal“-programmierbare Schnittstellenbausteine. Dieses Verfahren sei anhand der Embedded-Controller



ExC55 und ExC53 von Eckelmann kurz erläutert: Beide Controller-typen sind standardmäßig mit Ethernet-Schnittstelle ausgerüstet. Als Hersteller kauft Eckelmann MAC-Adressen für Ethernet-Schnittstellen, die eine eindeutige Identifizierung der mit dem entsprechenden Schnittstellen-Controller ausge-

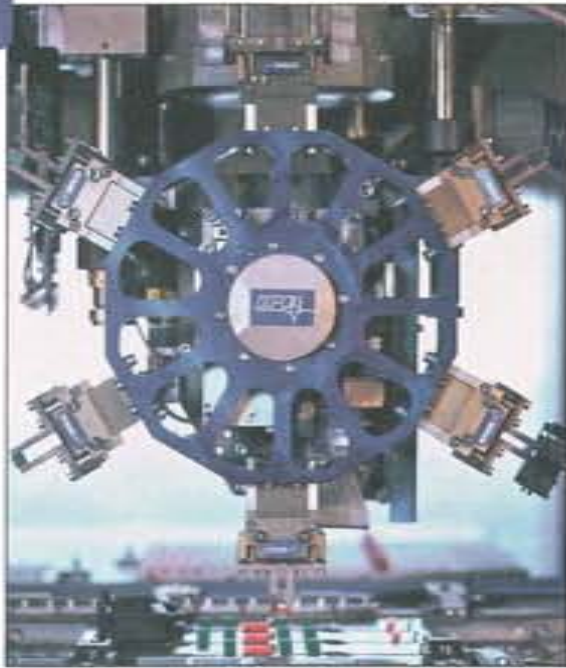
## USB - RS232, RS422, und RS485

- Konverter für Labor und Industrie
- einfache Installation, kleine Bauform, LEDs für Power, Rx, Tx
- USB-Treiber stellen virtuellen COM-Port zur Verfügung
- Stromversorgung über USB-Port
- aktive Endwiderstände und Echounterdrückung per Jumper konfigurierbar
- max. Baudraten bis 3 MBit/s
- galvanisch isoliert
- DIN-Schienen Montage möglich

Entwicklung, Herstellung und Vertrieb kundenspezifischer USB-Konverter

[www.NienTech.de](http://www.NienTech.de)

Tel.: 034721 / 24573



statteten Steuerung erlaubt. Die Steuerungs-Software fragt diesen Code ab und kooperiert nur mit der über die MAC-Adresse zugewiesenen Hardware. Da die MAC-Adresse neben einer laufenden Nummer einen Herstellercode und eine Produktartbezeichnung beinhaltet, ist der Aufbau von skalierbaren Verriegelungen möglich. Auch die Fernabfrage durch Maschinen- oder Steuerungshersteller ist möglich.

Bei Steuerungen ohne Ethernet-Schnittstelle erfolgt eine vergleichbare Verriegelung über Checksummen von Seriennummer und Vendor-ID, die im schreibgeschützten (Read-Only) Partitionen von nullspannungsfesten Flash-

In den SPS- oder Bahnsteuerungsprogrammen von Maschinen und Geräten stecken in Form von technologischem Know-how und Applikationserfahrung große immaterielle Vermögenswerte und ein strategisch wichtiger Wettbewerbsfaktor der Maschinen-Hersteller.

speichern hinterlegt werden. Die Hürde für das Kopieren ist bei dieser Lösung zwar hoch; unmöglich ist eine 1:1-Kopie der Software beziehungsweise Steuerung bei diesem Ansatz dennoch nicht. Das Kopieren des Hardware-Designs geht manchmal soweit, dass sogar Flashspeicher oder programmierbare Bausteine von der Originalplatine herunter gelötet, ausgelesen und kopiert werden.

Aus diesem Grund hat Eckelmann in enger Kooperation mit einem Maschinenbauer eine Lösung entwickelt, die praktisch 100-%igen Kopierschutz bietet: den CAN-Dongle.

## Das Dongle-Konzept

Die Idee, die hinter dem CAN-Dongle steckt, bedient sich einem Vorbild aus der PC-Welt. Die Bedrohung durch Raubkopien wurde dort schon viel früher relevant und von den großen Software-Hersteller auch erkannt. Zum Schutz ihrer Patente und des Know-hows, das in der PC-Software steckt, entwickelten sie die so genannten Hardware-Dongle. Dabei handelt es sich um Kopierschutzstecker, die auf gängige Schnittstellen wie USB oder Centronix aufgesteckt werden.



Dieses Konzept lässt sich ebenso auf die Welt der Maschinensteuerungen übertragen. Als Standard-Kommunikationssysteme sind dort unterschiedliche Feldbusse im Einsatz. Da Eckelmann seit langem den CAN-Bus als Standard-Kommunikationsstandard favorisiert, wurde das Dongle-Prinzip zunächst für dieses Bussystem umgesetzt. Es lässt sich aber ohne großen Aufwand auch auf andere Feldbus-Systeme wie zum Beispiel Profibus oder Devicenet übertragen.

Wie funktioniert nun ein solcher Feldbus-Dongle? Das Dongle ist ein selbstständiges Feldbus-Modul, das mit einem preiswerten 8-Bit-Prozessor ausgestattet ist und über den internen CAN-Bus mit der Steuerung kommuniziert. Die Steuerung selbst sendet nun eine Zahlenkombination, die im Dongle-Prozessor nach einer einprogrammierten mathematischen Formel verrechnet wird. Das Dongle schickt sein Ergebnis an die Steuerung zurück, die die Richtigkeit der mathematischen Transformation durch Vergleich mit selbst errechneten Werten überprüft. Entscheidend ist, dass der Prozessortyp des Dongles so ausgewählt wurde, dass die dort gespeicherte Firmware nicht auslesbar und somit auch nicht kopierbar ist.

Die Prüfreaktion lässt sich kundenspezifisch konfigurieren. So kann die Steuerung beispielsweise schon nach einmaliger Nicht- oder Fehlreaktion des Dongles den Betrieb abbrechen beziehungsweise in einen Sicherheitsmodus wechseln. Um seltenen, aber möglichen Übertragungsfehlern Rechnung zu tragen, ist auch eine beliebige Fehlertoleranz wählbar. Ein kopiertes Maschinenprogramm ist also nicht lauffähig, da die zyklische Freischaltung durch das Dongle nicht mitkopiert werden kann. Die Abfrageroutine lässt sich an verschiedenen Stellen des Steuerungsprogramms einbauen. Ein Auffinden oder gar Löschen dieser Routinen im Quellcode ist damit ausgeschlossen beziehungsweise derart aufwendig, dass der Kopierversuch unattraktiv wird.

Die einzige, aber unverhältnismäßig aufwendige Möglichkeit zum „Austrock-

Das Dongle ist ein selbstständiges Feldbus-Modul, welches über den internen CAN-Bus mit der Steuerung kommuniziert.

sen" der Donglefunktion wäre ein kontinuierliches Auslesen der von der Steuerung zum Dongle gesendeten Zahlenkombination sowie der zurückgesendeten Ergebnisse und einer numerischen/kombinatorischen Rekonstruktion der Umrechnungsformel. In Fällen, in denen sich – angesichts des Maschinenwertes – selbst dieses aufwendige Verfahren lohnen könnte, ist eine Steigerung der Dongle-Sicherung möglich. Sie besteht darin, die mathematische Formel zur Berechnung des Prüf-Ergebnisses zyklisch zu verändern. Dazu werden dem Dongle zusätzliche Rechenparameter aus einem steuerungseigenen Speicher (nur beschreibbarer write-only Flash-Speicher) übertragen. Die mathematische Formel, die der Dongle-Prozessor abarbeitet, setzt sich dann aus zwei Parametern direkt aus dem Prozessor des Dongle und weiteren bis zu sechs Parametern aus dem zusätzlichen Flash-Speicher zusammen. Diesen Zusatzspeicher kann der Maschinenbauer selbst zyklisch ändern. In diesem Fall kann nicht einmal mehr der Steuerungshersteller den Dongle-Code knacken. Für eine Überprüfung der ordnungsgemäßen Dongle-Funktion im Reklamationsfall kann der Hersteller den Dongle maximal in seinen Auslieferungszustand zurücksetzen.

Eine Rekonstruktion des letzten aktiven Schutz-Algorithmus ist selbst für den Hersteller des Dongle unmöglich. Ein Kopieren der Applikationssoftware des Controllers nützt also rein gar nichts. Selbst eine 1:1-Kopie von Maschine und Steuerung ist wertlos, da die Freigabe durch das CAN-Dongle nicht erfolgt.

### Unabhängig von der Steuerung

Das CAN-Dongle, welches zunächst für den Einsatz mit den Controllern ExC55 und Ex53 konzipiert wurde, ist nicht mit den Eckelmann-Steuerungen „verheiratet“. Das heißt: Jede Steuerung, die über einen CAN-Bus mit CANopen Protokoll V2.x verfügt, kann das Dongle ansprechen. Für den Betrieb werden lediglich eine 5-V-Gleichspannung und der CAN-Bus benötigt. Für den elektrischen Anschluss kann der 10-polige Gehäusebus verwendet werden. Als Gegenstecker empfiehlt sich der Combicon-Stecker von Phoenix Contact (Typ MC 1,5/10-

ST...). Rein softwaretechnisch erfolgt der Datenaustausch – also das Lesen und Schreiben des Dongles – über PDO-Transfer (Prozessdaten). Für die Programmierung eines neuen Sicherheitscodes muss die Steuerung auch den SDO-Transfer (Servicedaten) beherrschen. Für ungeübte Programmierer bietet Eckelmann Beispielprogramme in Codesys, einem IEC61131-3-kompatiblen Programmierwerkzeug an. gh

Nähere Informationen:  
info@eckelmann.de



Toni  
Schneider

ist tätig im Bereich  
Embedded Control Systems  
bei Eckelmann.

**Geht nicht,  
gibts nicht!**

bis 120°C

## SPEED7-CPU 317 mit integriertem High-Speed-EtherNET

Hardware: **Läuft auch unter Extrembedingungen**

- Arbeitsspeicher 512kByte erweiterbar bis 8MByte (jeweils 50% Programm/50% Daten)
- Ethernet-Interface für PG/OP-Kommunikation
- Profibus-DP-Master, 12MBAud, bis zu 125 Slaves
- zusätzlich integrierter EtherNET-CP 343 mit RFC1006, TCP/IP und UTP, projektierbar 16 (bis zu 256) Verbindungen
- SPEED-Bus für Highspeed I/O-Kommunikation
- MMC-Slot, Echtzeit-Uhr
- MPI-Interface mit 12 MBit/s

CPU 317SN/NET  
Bestell-Nr.: VIPA 317-4NE11

2.9



Mit Speed voraus – mit den VIPA SPEED7-CPU kommen Sie als er  
Die SPEED7-CPU sind weltweit die schnellsten mit STEP 7 von Sieme  
mierbaren CPUs. Bis zu 50.000 Anweisungen pro ms können bearbeite