Security-Anker ratsam: Verschlüsselungsverfahren schützen mithilfe kryptografischer Schlüssel die Software-Funktionen von Produkten.

3D-Druck schützt: Additive Fertigungsverfahren bieten Schutz vor Plagiaten.

Auftragsfälscher sind unterwegs: Die Fälscher können in Zusammenarbeit mit 3D-Fertigungszentren Produkte herstellen, die sich vom Original nicht unterscheiden.

Fotos: Wibu-Systems, Edler von Rabenstein, fotohansel, ristaumedia.de, iaremenko, Artur Marciniec, Ideeah Studio Manuel Adorf

FOKUS TECHNIK

Produktpiraterie – virtuellen Dieben das Handwerk legen

In Zeiten von Industrie 4.0 sind virtuelle Diebe besonders gefährlich. Sie erzeugen auf Basis digitaler Vorlagen identische Produkte, die sich vom Original nicht unterscheiden. VDMA-Mitglieder zeigen, wie sich Hersteller schützen können.

→ Sie brechen keine Schlösser auf, schlagen keine Fenster ein und klettern über keine Zäune. Trotzdem sind sie gefährlicher als jeder Einbrecher: Die Rede ist von Hackern, die als clevere virtuelle Diebe und Spitzel in die IT-Systeme der Industrie eindringen. Eine Umfrage bei VDMA-Mitgliedern zu erfolgreichen Gegenmaßnahmen zeigt auf, wie sich die Industrie absichern kann.

Auftragsfälscher haben sich etabliert

Die Gefahr des Datenklaus wächst mit Industrie 4.0, denn Industrie 4.0 bringt neue Bedrohungen mit sich. Wenn Produktpiraten etwa digitale Vorlagen für den 3D-Druck in die Hände fallen, können sie identische Teile erzeugen, die nicht mehr als Plagiate erkennbar sind. So gibt es bereits Auftragsfälscher, die mit darauf spezialisierten 3D-Fertigungszentren kooperieren.

„Digitale Vorlagen, Software in Anlagen und zentrale Datenbanken werden das bevorzugte Angriffsziel“, warnt VDMA-Präsident Dr. Reinhold Festge im Vorwort zur neuen Produktpiraterie-Studie der Arbeitsgemeinschaft Produkt- und Know-how-Schutz im VDMA. Er empfiehlt dringend, in digitale Schutzmaßnahmen gegen Produktpiraten zu investieren.

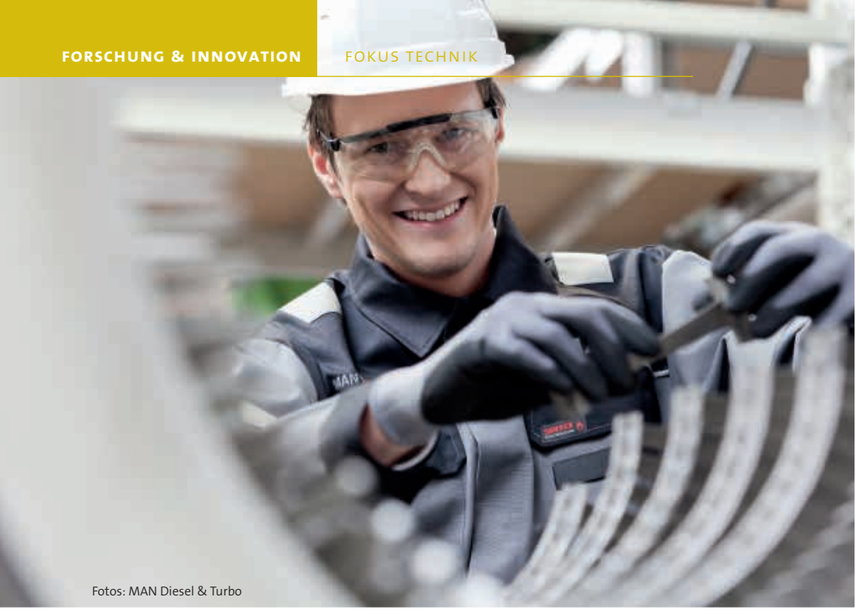
Know-how-Schutz ernst nehmen

Zustimmung kommt von Oliver Winzenried, Vorstand und Gründer der Karlsruher Wibu-Systems AG. Mit Interesse und viel Aufmerksamkeit beobachtet er den Trend zu Industrie 4.0: Als positiv sieht der Vorstandsvorsitzende der Arbeitsgemeinschaft Produkt- und Know-how-Schutz „Protect-Ing“ im VDMA an, dass Produkte bei einheitlicher Hardware „durch Konfiguration der Software und Parameter unterschiedliche Funktionen ausführen können, sich im Feld aktualisieren und aufrüsten lassen und dadurch für Hersteller neue Geschäftsmodelle entstehen“. Doch mit der zunehmenden Funktionalität wachse die Notwendigkeit, die Daten und Informationen über die Entwicklung und Herstellung dieser Produkte zu schützen. „Diese Erkenntnis kommt auch bei unseren Kunden in der Automatisierungstechnik und im Maschinen- und Anlagenbau an“, berichtet Winzenried. „Wir sind an einigen Forschungs- und Entwicklungsprojekten zu diesem Thema in Deutschland beteiligt und die führenden Maschinenbauer nehmen sie sehr ernst.“

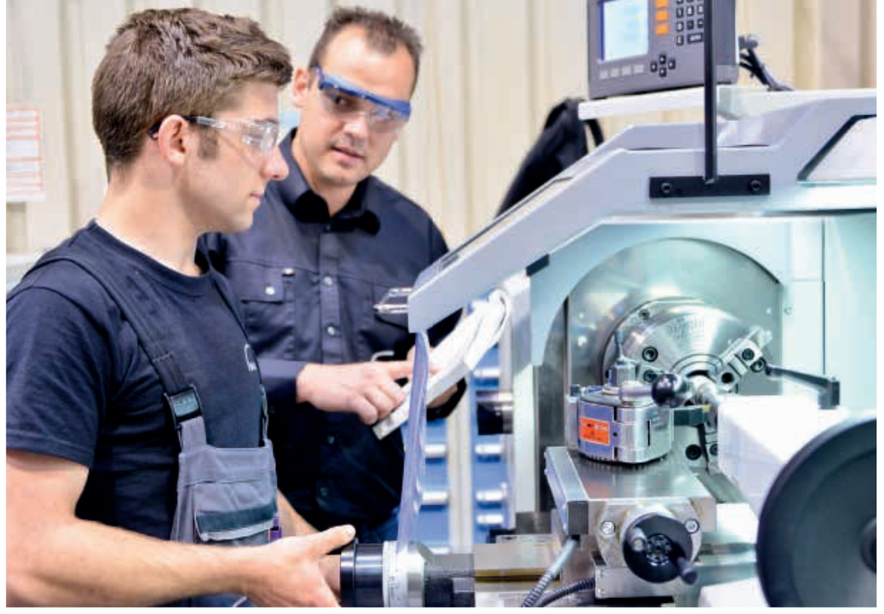
Traceability ist ein Mittel zum Zweck

Der Experte empfiehlt Herstellern eine vom Produkt abhängige Mischung an Maßnahmen zum Produkt- und Know-how-Schutz. Gefragt sei einerseits Schulung und „Awareness der Mitarbeiter“, damit sie sich über die zu schützenden Werte im Klaren sind und damit nicht eine Vielzahl von Zulieferern komplette Produktionsdetails für deren Angebotsabgabe erhalten. Andererseits seien auch rechtliche und technische Schutzmaßnahmen nötig. Ein Mittel zum Zweck sei Traceability, die Rückverfolgbarkeit der Produkte im Produktions- und Vertriebsprozess. „Traceability bietet Mehrwert in der Logistik und kann für Plausibilitätsprüfungen genutzt werden“, sagt Winzenried. „So kann der Anwender mithilfe von pfiffiger Kennzeichnung Originale von Plagiaten unterscheiden.“

Daneben sei präventiver Schutz wichtig. Als Verschlüsselungsverfahren zum Schutz der Software-Funktionen in Produkten empfiehlt Winzenried Security-Anker, die kryptografische Schlüssel sicher speichern und nicht kopiert werden können. All diese Schutzmaßnahmen erschweren seiner Ansicht nach den Nachbau und die Produktpiraterie. Er rät vor allem dann dringend zum Einsatz, wenn in Geräten (Stichwort: Internet of Things) und Maschinen digitale Produktionsdaten, Parameter und Embedded Software vorkommen. →



Fotos: MAN Diesel & Turbo



Manche Unternehmen besitzen eine eigene Cloud, auf der sie sensible Maschinen- und Sensordaten zum Beispiel der Motoren ihrer Kunden speichern ... ... und auswerten.

Laut der VDMA-Studie „Produktpiraterie 2016“, die im April 2016 veröffentlicht wurde, ist Reverse Engineering zu 70 Prozent die Hauptursache für erfolgreiche Produktpiraterie. Als Gegenmaßnahme habe sich hier die Embedded Security bewährt – eingebettete IT-Systeme mit Schutzfunktionen (wie Verschlüsselung). „Unter Security verstehe ich den Schutz vor Manipulation“, erklärt Winzenried. „Hierzu werden elektronische Signaturen und asymmetrische Kryptografie verwendet, damit die Systeme selbst prüfen können, ob Software und Daten unverändert sind und von einem berechtigten Herausgeber kommen.“ Zudem sei es wichtig, dass alle vernetzten Geräte in einer intelligenten Maschine oder Anlage eine fälschungssichere Identität bekommen. Zwingend erforderlich sei diese Security bei den immer offeneren Netzen. Hier könne Embedded Security einen wichtigen Beitrag dazu leisten, dass die Schutzmaßnahmen auch zuverlässig funktionieren.

„Anwender können mithilfe von pfiffiger Kennzeichnung Originale von Plagiaten unterscheiden.“

Foto: Wibu-Systems

Oliver Winzenried
Wibu-Systems

Geistiges Eigentum schützen

Wie das in der Praxis ablaufen kann, zeigt ein Blick auf zwei typische Einsatzfälle: Ein Hersteller aus der Textilindustrie schützt seine Maschinen vor dem Nachbau, indem er den Zugriff auf die Embedded Software in der Steuerung verhindert, in der wichtiges Know-how steckt – etwa zum besonders schnellen und qualitativ hochwertigen Besticken von Textilien. „Ferner können die Maschinen geschützte Produktionsdaten, sogenannte Punch-Daten, verarbeiten. Auf diese Weise lassen sich nicht nur das Know-how des Maschinenbauers, sondern mit den Produktdaten auch das geistige Eigentum der Kunden schützen“, sagt Winzenried.

Das System erfasse aber auch die Anzahl der produzierten Lose, um zu verhindern, dass jemand mit Original-Produktionsdaten in einer Textilfabrik unbemerkt in einer Sonderschicht auf eigene Rechnung Produkte für den Graumarkt herstellt.

Das zweite Beispiel stammt aus der Automatisierungstechnik. Embedded Security dient bei speicherprogrammierbaren Steuerungen (SPS) zum Konfigurieren der SPS-Funktionen. Diese Maßnahme erleichtert dem Steuerungshersteller den Verkauf und ermöglicht eine Exportkontrolle von genehmigungspflichtigen Funktionen. „Es kommt auch in der Entwicklungsumgebung der Steuerungen zu einem Know-how-Schutz des Maschinen- oder Anlagenbauers“, erläutert Winzenried. Für den weltweiten Service seien diese Maßnahmen und die Integration der Vergabe von Zugangsrechten in den Geschäftsprozess sehr wichtig.

Sichere Übertragungskanäle

Mit Industrie 4.0 und den Folgen beschäftigt sich seit Jahren auch Michael Wenninger, Senior Business Development Manager bei der MAN Diesel & Turbo SE aus Augsburg. „Im Zuge der Digitalisierung der Wertschöpfungskette hat sich der fast ausschließliche Datentausch über digitale Medien etabliert. Damit gestalten sich Alltagsprozesse effizienter und komfortabler. Mit Blick auf die Datensicherheit birgt das jedoch auch Risiken“, sagt Wenninger. Für den Anwender sei es wichtig, auch die Übertragungskanäle zu sichern. Daher haben die Augsburger unter dem Begriff Online-Service eine eigene Cloud installiert, auf der sie sensible Maschinen- und Sensordaten etwa der Motoren ihrer Kunden speichern und auswerten. Das geschieht zum Beispiel im Rahmen der vorausschauenden Wartung und Instandhaltung.

„Für die Datenübertragung nutzen wir nach dem Prinzip des sogenannten Virtual Private Network einen eigenen, gesicherten Daten-Tunnel“, erklärt Wenninger. „Weil das aber nicht zu unserer Kernkompetenz zählt, bedienen wir uns hier bei den Spezialisten der entsprechenden Industrie, die für die sichere Technologie sorgen.“ Der MAN-Manager empfiehlt den Einsatz von branchenweiten Standards. Für eine effiziente Interoperabilität über Unternehmens- und Ländergrenzen hinweg und für Wettbewerbsfähigkeit im vernetzten Marktumfeld bilden diese einen nachhaltigen Unterbau.

Foto: MAN Diesel & Turbo

„Für den Anwender ist es wichtig, auch die Übertragungskanäle zu sichern.“

Michael Wenninger
MAN Diesel & Turbo

Produkte eindeutig identifizieren

Zum direkten Schutz vor Plagiaten empfiehlt Wenninger die eindeutige Identifikation eines Produkts mit einer Automationstechnologie, die sich auch für Anwendungen aller Art in der Logistik, der Supply Chain und im Ersatzteilvertrieb nutzen lässt. Es handle sich um ein flexibles Verfahren, das eine Vielzahl von Maßnahmen und Funktionen biete. Auf diese Weise könne ein Scanner etwa mithilfe eines maschinenlesbaren DataMatrix-Codes, des wahrscheinlich bekanntesten 2D-Codes, Bedienungsanleitungen abrufen oder ein Produkt eindeutig per Seriennummer identifizieren. Hier komme die Traceability ins Spiel. „Dank des DataMatrix-Codes können wir einzelnen Komponenten unserer Motoren jeweils unterschiedliche und sehr individuelle Informationen – zum Beispiel über den Verschleiß – zuordnen“, sagt Wenninger. „Auf diese elegante Art und Weise erhalten wir auch eine wertvolle Rückmeldeschleife für unsere Entwicklung.“

Ziel der Kombination von Traceability und DataMatrix-Code sei für MAN Diesel & Turbo in erster Linie die einfache Identifizierung korrekter Bauteile. „Uns geht es vor allem darum, die Beeinträchtigung der Anlagenverfügbarkeit und Betriebssicherheit durch fehlerhafte Bauteile zu vermeiden. Wichtig ist uns, die hohe Qualität und Langlebigkeit unserer Produkte sicherzustellen“, erklärt Wenninger.

Produktschutz mit RFID

Auch vielen Unternehmen des Maschinenbaus „droht die Gefahr durch Produktpiraterie“, denkt René Steiner, Business Development Manager RFID bei der Hans Turck GmbH & Co. KG aus Mülheim an der Ruhr. So gebe es einen Trend, vor allem wichtige →

Foto: Wibu-Systems

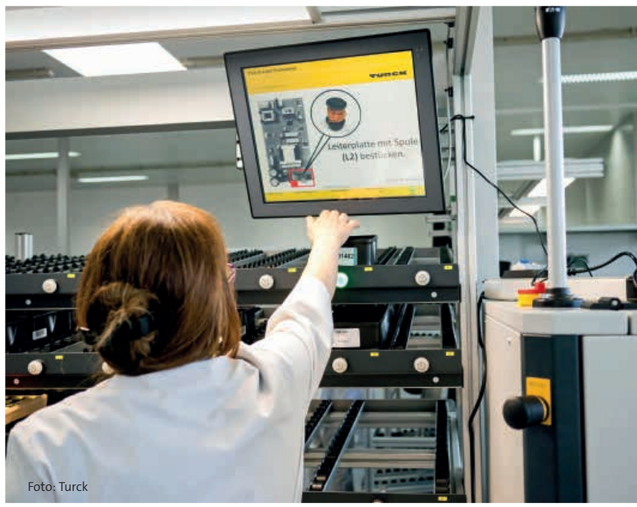


Foto: Turck

Datenschutz gelingt, indem Firmen den Zugriff auf die Embedded Software verhindern oder Daten mit der UID verschlüsseln.

„Das Ausstatten wichtiger Maschinenteile mit RFID erhöht den Mehrwert der Maschine.“

Foto: Turck

René Steiner
Turck

Maschinenteile mit RFID-Funkdatenträgern auszustatten. „Dieses sogenannte Tagging erhöht den Mehrwert einer Maschine“, erklärt Steiner. Die Steuerung einer Maschine könne etwa beim Wechseln einer Walze gleich die zugehörigen Kennwerte aus dem integrierten RFID-Datenträger automatisch einlesen.

Daten per UID verschlüsseln

Zum Schutz der sensiblen Daten empfiehlt Steiner neben dem optionalen Passwort eine Verschlüsselung der Daten mit der jeweiligen Unique Identification Number (UID) und einem zusätzlichen individuellen Schlüssel in dem überlagerten System. Somit lassen sich die Daten zwar auf einen anderen Datenträger kopieren, verlieren aber aufgrund der fehlenden Schlüssel ihre Gültigkeit.

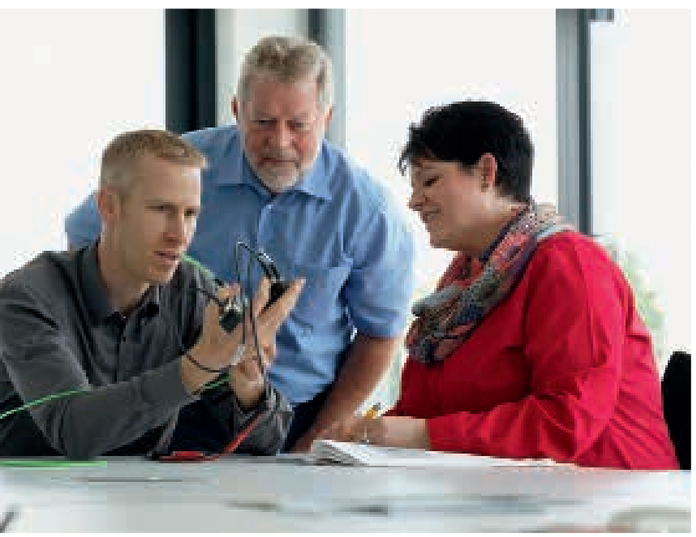
Zusätzlich gebe es die Möglichkeit, den Datenträger durch eine spezielle unsichtbare Markierung individuell zu kennzeichnen. All diese Maßnahmen würden dazu beitragen, dass nur noch Experten mit dem entsprechenden Know-how und dem richtigen Equipment ein elektronisches Bauteil eins zu eins kopieren können.

In der Praxis hat sich diese Vorgehensweise bereits mehrfach bewährt. So bestückt ein Turck-Kunde seine Bandfilter bereits mit RFID-Chips. „Die Maschinensteuerung liest den Chip aus und warnt vor dem Einsatz von falschen Filtern“, berichtet Steiner. Der Einsatz der Filter werde auch im elektronischen Logbuch der Maschinen gespeichert. Das schaffe Transparenz sowohl beim Maschinenhersteller als auch beim Endkunden im Falle einer Reklamation.

Für den Endkunden bedeute dies zusätzlich, dass eine Gefährdung von Personen und Maschinen wegen des Einsatzes minderwertiger oder gefälschter Ersatzteile vermieden wird. Auch Walzen oder Stanzmesser enthalten mittlerweile RFID-Chips, mit denen sich das Bauteil eindeutig identifizieren lasse. Die Elektronik erlaube dem Kunden nicht nur die sichere Identifikation, sondern das Erfassen und Speichern wichtiger Kennwerte und Produktionsdaten beispielsweise zur Wartung.

Potenzial für Cyber-Attacken

„Industrie 4.0 bietet großes Potenzial für Innovationen, birgt aber auch zahlreiche neue Angriffsmöglichkeiten für Cyber-Attacken“, beobachtet auch Christoph Plass, Vorstand der Unity AG aus Paderborn. Angreifer würden keinen physischen Kontakt mehr zu Systemen benötigen, um geistiges Eigentum zu entwenden. Insbesondere die Zugänge zu den IT-Systemen und die Kommunikationsverbindungen bieten seiner Ansicht nach viele neue Schwachstellen: Sie müssen daher abgesichert werden.



Fotos: Turck

Dank neuer Elektronik kann der Kunde sein Produkt nicht nur sicher identifizieren, sondern auch wichtige Produktionsdaten erkennen und erfassen.

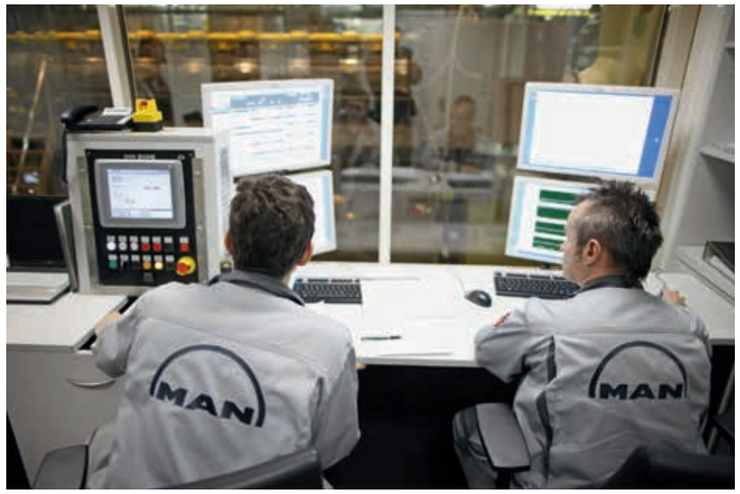


Foto: MAN Diesel & Turbo

Der Datentausch über digitale Medien birgt auch Risiken, denen Hersteller präventiv begegnen sollten.

Hinzu komme, dass intelligente technische Systeme größtenteils nur dann entwickelt werden können, wenn die Vernetzung der Hersteller und ihrer Partner (Lieferanten) zunimmt. Erfolgreiche Zusammenarbeit setze aber auch den Austausch von technischen Daten wie beim 3D-Druck oder bei Predictive Maintenance voraus. Es gelte daher, die technologischen Erfindungen vor Produktpiraterie oder Diebstahl zu schützen. „Präventive Maßnahmen zum Schutz des geistigen Eigentums sind daher proaktiv in Strategien, Prozesse, Produkte und Systeme zu integrieren“, empfiehlt Plass.

Foto: Unity

„Unternehmen sollten geistiges Eigentum proaktiv und vorbeugend schützen.“

Christoph Plass
Unity

Datenzugang einschränken

Die ideale Schutzmaßnahme für Unternehmen sei die Kombination von rechtlichem, organisatorischem und technischem Schutz. Zu den rechtlichen Maßnahmen gehören Patente und Geschmacksmuster. „Leider ist ein Schaden schon entstanden, bevor diese Maßnahmen wirken“, sagt Plass. Jeder Hersteller sollte deshalb zusätzlich die für ihn geeigneten technischen Schutzsysteme wählen, um vorbeugend Produktpiraterie abzuwehren. Dies könnten Kennzeichnungstechnologien, Track und Trace und präventiver Schutz für Software und Know-how sein. Unternehmen sollten sich auch über Angriffe von innen und über die Kooperation mit Zulieferern Gedanken machen und neben Konzepten wie Zutrittskontrolle sensible Informationen und Daten nur bestimmten Personen zugänglich machen.

Sichere Identität ist zentral

Um den Schutz intelligenter technischer Systeme sicherzustellen, müssen die Herausforderungen an den Systemschutz aufgenommen und berücksichtigt werden. „Hierfür leistet das Projektteam der Nachhaltigkeitsmaßnahme ‚Prävention gegen Produktpiraterie – itsowl-3P‘ →

INFO

Produktpiraterie – Gegenmaßnahmen in Angriff nehmen

Wie aus der aktuellen VDMA-Studie zum Thema Produktpiraterie hervorgeht, nehmen Produktfälschungen Jahr für Jahr zu. Der entstandene Schaden für Hersteller wurde im Jahr 2015 auf 7,3 Milliarden Euro in Form entgangener Einnahmen geschätzt. Mit 62 Prozent werden am häufigsten Komponenten gefälscht, aber auch vor ganzen Maschinen machen die Plagiatoren nicht halt.

Der Anteil an gefälschten Maschinen liegt bei 41 Prozent. Bei den verletzten gewerblichen Schutzrechten steht mit 41 Prozent die Patentverletzung an erster Stelle, gefolgt von Markenverletzungen mit 36 Prozent. Von Gefahren für den Menschen berichten 39 Prozent der Hersteller, etwa auf Kundenseite in der Nahrungsmittelindustrie oder bei Industriearmaturen.

Informationen über Produktpiraterie und geeignete Gegenmaßnahmen liefern VDMA-Informationsveranstaltungen und VDMA-Publikationen.

LINKS

Infotag Industrial Security 2016
pks.vdma.org/article/-/article-view/13073670

Industrie-4.0-Security
industrie40.vdma.org/article/-/article-view/12339452

Studie Produktpiraterie 2016
pks.vdma.org/article/-/article-view/13069313

Branchenführer Produkt- und Know-how-Schutz
pks.vdma.org/article/-/article-view/13086951

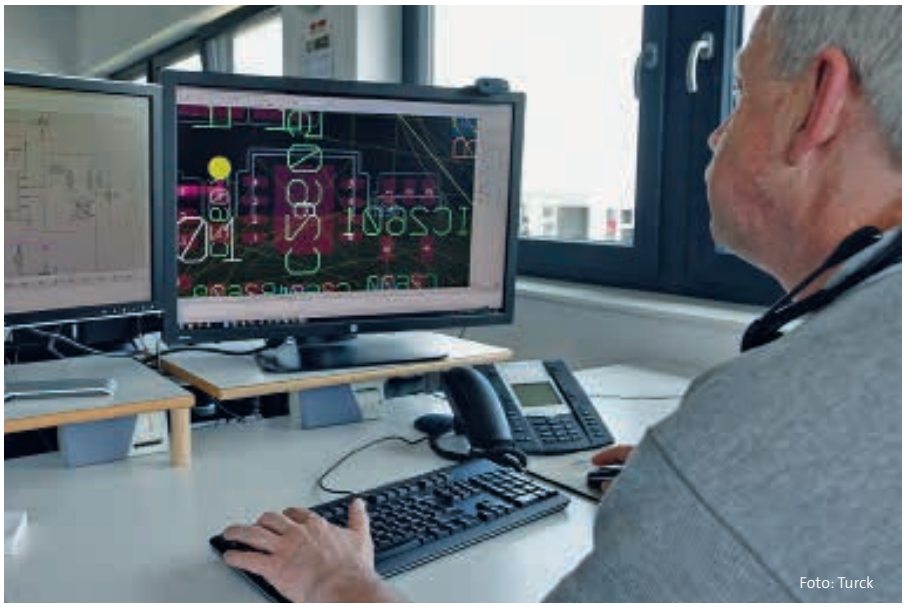


Foto: Turck

Die Maschinensteuerung kann alle zugehörigen Kennwerte aus dem RFID-Datenträger einlesen.

des Spitzenclusters ‚it's OWL' einen entscheidenden Beitrag", berichtet Plass. Die erarbeiteten Empfehlungen über das Cluster-Management werden Unternehmen zur Verfügung gestellt. Wichtig sei eine sichere Identität, die nicht manipuliert, gefälscht oder missbraucht werden kann. Eine Software-Verschlüsselung reiche als Schutz gegen Angriffe auf Maschinencodes nicht aus. Idealerweise sei der Software-Schlüssel in einer speziell geschützten Hardware abgelegt, die weder auslesbar ist noch manipuliert werden kann.

3D-Druck kontra Produktpiraterie

Als eine Möglichkeit zum Schutz vor Plagiaten empfiehlt Plass additive Fertigungsverfahren, häufig als 3D-Druck bezeichnet. So habe ein Spezialist für Aquariumsbeleuchtungen und Wasserpflege per Lasersintern ein neuartiges Pumpenrad entwickelt. „Diese Fertigungstechnologie ermöglichte den Entwicklern völlig neue Gestaltungsmöglichkeiten und bietet dem Unternehmen besondere Vorteile gegenüber Produktfälschern", sagt Plass.

AUTOR
Nikolaus Fecht
Freier Journalist, Gelsenkirchen

KONTAKT
Steffen Zimmermann
VDMA Produkt- und Know-how-Schutz
Telefon +49 69 6603-1978
steffen.zimmermann@vdma.org

LINKS
pks.vdma.org/security
www.protect-ing.de
www.i40-security.de

PROFILE

MAN Diesel & Turbo SE, Augsburg
Der weltweite Anbieter von Großdiesel- und Gasmotoren sowie Turbomaschinen für maritime und stationäre Anwendungen entwickelt Zweitakt- und Viertaktmotoren. Die Motoren arbeiten im Leistungsbereich von 450 Kilowatt bis 87 Megawatt. Im Unternehmen entstehen außerdem Gas- und Dampfturbinen sowie Kompressoren.
Umsatz: 3,3 Milliarden Euro, Mitarbeiter: 15 000

Unity AG, Paderborn
Das Unternehmen ist eine Managementberatung für zukunftsorientierte Unternehmensgestaltung. Seit über 20 Jahren zählen Firmen aus der Automobilindustrie, Luft- und Raumfahrt, Gesundheitswirtschaft und Medizintechnik, Energie-, Pharma- und Chemieindustrie sowie der produzierenden Industrie zu den Kunden. Umsatz: 28,5 Millionen Euro, Mitarbeiter: 210

Hans Turck GmbH & Co. KG, Mülheim an der Ruhr
Der Sensor-, Feldbus-, Anschlusstechnik- und Interfaceanbieter ist spezialisiert auf Lösungen für die Industrieautomation. Das Familienunternehmen bietet mehr als 15 000 Produkte aus der Sensor-, Feldbus-, Anschluss- und Interfacetechnik sowie RFID für die Fabrik- und Prozessautomation. Umsatz: 500 Millionen Euro, Mitarbeiter weltweit: 4 000

Wibu-Systems AG, Karlsruhe
Der Anbieter entwickelt seit 1989 sichere Hard- und Softwaretechnologien für das Digital Rights Management (DRM) von Software und Dokumenten. Diese Technologie bietet Kopier- und Know-how-Schutz, Lizenzierung und Security – von Embedded- und SPS-Systemen über Personalcomputer bis hin zur Cloud. Wibu-Systems zählt heute nach eigenen Angaben zu den größten Anbietern für Software- und Dokumentenschutz.
Mitarbeiter: 110

LINKS
www.dieselturbo.man.eu
www.turck.com
www.unity.de
www.wibu.com