DOI 10.2195/LJ_PROC10_Durchholz

Dokumentierte Authentifizierung als wirksamer Schutz vor Produktpiraterie für Komponenten im Maschinen- und Anlagenbau

Dipl.-Ing. Janina Durchholz, Dipl.-Wi.-Ing. Dominik Stockenberger,
Prof. Dr.-Ing. Dipl.-Wi.-Ing. Willibald A. Günthner
Technische Universität München
Lehrstuhl für Fördertechnik Materialfluss Logistik

Abstract: Das im Forschungsprojekt ProAuthent entwickelte Produktpiraterie-schutzsystem verknüpft zwei erfolgreiche Ansätze aus Logistik und Markenschutz. Durch die Verbindung von Funktionen des Tracking & Tracing und sicheren Kennzeichnungstechnologien entsteht ein effektives Konzept zum präventiven Schutz von Ersatzteilen und Komponenten im Maschinen- und Anlagenbau. Bauteile, die mit RFID gekennzeichnet sind, können so auf dem Weg durch die logistische Kette verfolgt und von autorisierten Lesegeräten auf ihre Echtheit hin geprüft werden. Ein Verfahren auf Basis einer kryptographischen Signatur macht aus einem einfachen passiven Logistiktransponder eine fälschungssichere Originalitätsmarkie-rung. Vier Pilotanwendungen im Maschinenbau zeigen die Funktionsweise des Systems gegen Produktpiraterie.

1 Problemstellung

1.1 Produktpiraterie im Maschinen- und Anlagenbau

Produktpiraten machen auch vor Investitionsgütern wie Maschinen und Anlagen nicht Halt, denn hier können Kopierer beachtlich von fremder Entwicklungsleistung profitieren und mit gefälschten Komponenten, Ersatzteilen und ganzen Maschinen lukrative Geschäfte machen. Im deutschen Maschinen- und Anlagenbau schätzt der VDMA den entstehenden Schaden auf sieben Milliarden Euro pro Jahr. Zwei von drei befragten Unternehmen gaben an, von Produktpiraterie betroffen zu sein; zudem gehen Schätzungen vom Verlust zehntausender Arbeitsplätze aus. [VDM08], [BMB10]

In der globalisierten Welt ist wirtschaftlicher Erfolg auf das Engste verknüpft mit der Fähigkeit zur kontinuierlichen Weiterentwicklung und Innovation. Aus diesem Grund sind Wissen und Know-how entscheidend für die Zukunft von Unternehmen. „Geistiges Eigentum, Know-how und starke Marken sind heute die Kronjuwelen erfolgreicher Unternehmen.“ [ICC06, S. 42]

Ein großer Teil dieses Know-hows befindet sich – teils offensichtlich, teils versteckt – in den Produkten eines Unternehmens. Es steckt in den Maßen, Fertigungsverfahren, Materialien, der Konstruktion und Funktionsweise jeder Komponente. Dieses Wissen zu schützen, stellt eine ganz besondere Herausforderung dar, da die Produkte zwangsläufig das Unternehmen verlassen, um

zum Kunden und damit in den Markt zu gelangen. Ein Schutz, der auf Geheimhaltung beruht, ist insbesondere bei den technischen Produkten, Ersatzteilen und Komponenten im Maschinen- und Anlagenbau ausschließlich in Teilbereichen möglich. Auch juristische Mittel können nur unterstützen, da sie vor allem reaktiv wirken, d.h. wenn die Produkte bereits kopiert und meist schon beim Kunden im Einsatz sind.

Präventiver Piraterieschutz für Produkte und Komponenten umfasst deshalb auf jeden Fall neben juristischen und organisatorischen Mitteln auch technische Maßnahmen, die möglichst früh in den Produktentwicklungsprozess eingebunden werden sollten. Hier gilt es systematische Vorgehensweisen zu entwickeln, die vielen Unternehmen heute noch fehlen, um Produktpiraterie effektiv zu begegnen und die Forschungs- und Entwicklungsleistung in ihren Produkten und den einzelnen Komponenten zu schützen. [WAB+07], [BMB10]

1.2 Forschungsansatz

Ein wirksamer technischer Schutz vor Piraterie entsteht durch die Kennzeichnung von Komponenten und eine konsequente Prüfung der Echtheit. Heute existieren im Wesentlichen zwei Ansätze aus Logistik und Markenschutz, um Fälschungen zu entdecken und so gegen Produktpiraterie vorzugehen:

1. Durch logistische Tracking&Tracing-Funktionen, die über den Weg eines individualisierten Produkts durch die Wertschöpfungskette Auskunft geben, kann ein Produkt datentechnisch verfolgt und rückverfolgt werden. Wertet man die Spur, die ein Bauteil in einem solchen System hinterlässt, systematisch aus, so lassen sich Unregelmäßigkeiten identifizieren, die ein Hinweis auf Produktpiraterie sind. Vorsicht ist z.B. geboten, wenn es keinen Datenbankeintrag über diese Seriennummer beim angeblichen Hersteller gibt, oder wenn die logistische Kette Lücken aufweist. [GS10], [RGO08]
2. Die Verwendung fälschungssicherer Merkmale zur Markierung echter Produkte und die oftmals manuelle Prüfung der Originalitätsmarkierung vor Ort haben primär die Aufgabe, Original und Fälschung unterscheidbar zu machen. Auf dieser Basis können Kopien identifiziert und Maßnahmen ergriffen werden. So wird z.B. der Kunde in die Lage versetzt, bestimmte Bauteile selbst zu prüfen und daraufhin zu entscheiden, ob er das Bauteil einsetzt oder nicht. [RGO08], [GS08], [ICC06, S.7]

Da beide Vorgehensweisen umfassende Vorteile haben, hat es sich das Konsortium des Forschungsprojekts ProAuthent[1] zur Aufgabe gemacht, ein integriertes

[1] Das Forschungsprojekt „ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau“ wird vom Bundesministerium für Bildung und Forschung gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Projektlaufzeit: Januar 2008 bis Januar 2011

Produktpirateriesschutzsystem zu entwickeln, welches die positiven Eigenschaften verbindet und optimal auf die Bedürfnisse des Maschinen- und Anlagenbaus eingeht.

Entscheidend ist in dieser Branche, in welcher v.a. Komponenten und Ersatzteile von Produktpiraterie betroffen sind, die Möglichkeit der Originalitätsprüfung vor Ort, ohne die Notwendigkeit eines Datenbankabgleichs (vergleiche dazu [GS08]). Gleichzeitig ist die Speicherung der Produkthistorie beim Maschinenhersteller notwendig, um aktiv und effektiv gegen Piraterie vorzugehen.

2 Dokumentierte Authentifizierung mit RFID

Als Teil der Ergebnisse des Forschungsprojekts wird in diesem Abschnitt die Anwendung der RFID-Technologie zur dokumentierten Authentifizierung von kritischen Komponenten im Maschinen- und Anlagenbau vorgestellt.

2.1 Authentifizierung

Kern des hier vorgestellten Schutzsystems ist die Authentifizierung, d.h. die Echtheitsprüfung, entscheidender, schützenswerter Bauteile während ihrer Lebensdauer, d.h. von der Produktion bis zur Verschrottung. Doch die Markierung einzelner Produkte und die spätere Prüfung der Merkmale sind stets mit Aufwand und Kosten verbunden. Deshalb ist es im Maschinen- und Anlagenbau nicht zielführend, prinzipiell jede Komponente einer Maschine mit einem Sicherheitsmerkmal auszustatten und dieses später automatisiert oder manuell auf Originalität zu prüfen. Der Aufwand wäre weit größer als der Nutzen. Ausschließlich jene Bauteile zu schützen, bei denen Nachahmungen und Kopien bekannt sind, greift jedoch zu kurz. Denn Ziel muss es sein, aktiv gegen Produktpiraterie vorzugehen, Fälscher im Vorfeld abzuwehren und das Kopieren unattraktiv zu machen.

Daher ist eine bauteilbezogene Risikoanalyse notwendig, in der jene Bauteile identifiziert werden, die von Nachahmung bedroht und gleichzeitig von besonderem Interesse für den Originalhersteller sind. Die einerseits interessant sind für Nachahmer und andererseits werthaltig und wichtig für den Originalhersteller. Die schützenswerten Bauteile liegen also in der Schnittmenge und erfüllen die Eigenschaften aus beiden Bereichen (vgl. Abbildung 1).

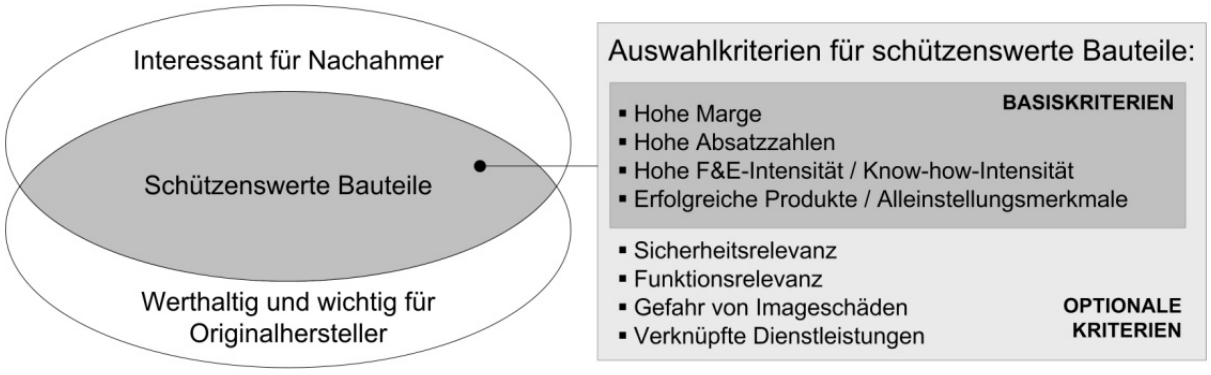

Abbildung 1: Auswahlkriterien für schützenswerte Bauteile

Sie zeichnen sich durch eine hohe Marge, hohe Absatzzahlen sowie aufwändige Forschungs- und Entwicklungsarbeit aus und haben bestimmte Alleinstellungsmerkmale, die sie zu erfolgreichen Produkten auf dem Markt machen. In Ergänzung können weitere Kriterien hinzugezogen werden, um klar die Komponenten zu bestimmen, die vorrangig durch Kennzeichnung und Authentifizierung vor Produktpiraterie geschützt werden sollen. Im Sinne des Produktpirateriesschutzes sollten natürlich möglichst viele Produkte gekennzeichnet sein, doch es gilt stets Kosten und Nutzen abzuwägen. Je besser die Informationen über die Schäden und Gefahren im Unternehmen durch Produktpiraterie sind, desto bewusster und sicherer kann die Entscheidung getroffen werden, welche Bauteile aktiv über eine Kennzeichnung geschützt werden sollen.

Die *sichere* Feststellung der Originalität einer Komponente basiert stets auf der Fälschungs- und Kopiersicherheit eines Merkmals sowie der manipulationssicheren Verbindung zwischen Kennzeichen und Produkt. Die Schutzwirkung entsteht in erster Linie aus der Tatsache, dass ein Pirat das Merkmal nicht (in ausreichender Genauigkeit und Qualität) reproduzieren kann. Zusätzlich muss unbedingt sichergestellt sein, dass das echte Merkmal nicht von einem Produkt auf ein zweites übertragen werden kann. Bei beiden Punkten ist nicht unbedingt eine 100-prozentige Sicherheit wichtig. Es gilt die Hürden zu erhöhen und den Aufwand für den Fälscher so zu steigern, dass das Kopieren unrentabel oder nicht ausreichend gewinnbringend betrieben werden kann.

Aus diesem Grund sind AutoID-Technologien nur bedingt für diese Aufgabe geeignet. Sie können ein Bauteil individualisieren und damit einzigartig und unterscheidbar machen. Fälschungsschutz ist jedoch zunächst nicht gegeben. Deshalb wurde die Anwendung von RFID derart weiterentwickelt, dass Kopiersicherheit auf Basis eines einfachen passiven Transponders möglich ist.

Die Aussage über die Echtheit des Transponders und damit des Bauteils wird nicht durch die Prüfung der Plausibilität von Datenbankeinträgen getroffen, sondern aufgrund der auf dem Transponder gespeicherten Daten, die nur mit Hilfe eines kryptographischen Schlüssels erzeugt werden können. Um ein Klonen von Transpondern, also ein Anfertigen von 1:1-Kopien zu verhindern, wird die eindeutige, vom Chiphersteller vergebene Tag-ID (auch: UID) des RFID-Chips mit einbezogen. Es kommt ein asymmetrisches Verschlüsselungsverfahren zum Einsatz, welches die eindeutige Identifikationsnummer des Bauteils (EPC, Elektronischer Produktcode) und die einmalige Tag-ID des Chips zu einer Signatur verschlüsselt, die im freien Speicherbereich des Transponders abgelegt wird. Dieser Schritt geschieht direkt im Anschluss an die Produktion des Bauteils beim Hersteller mit Hilfe eines privaten Schlüssels, der unbedingt vor fremdem Zugriff geschützt werden muss (Abbildung 2). Beim Prüfen wird die Signatur auf dem Transponder unter Verwendung des zugehörigen öffentlichen Schlüssels wieder decodiert. Die resultierende Identifikationsnummer des Bauteils und die ID des Chips müssen dann mit den auf dem Transponder gespeicherten Daten übereinstimmen, damit der RFID-

Transponder und damit das Bauteil original sind. Der Authentifizierungsprozess findet innerhalb der Software des RFID-Lesegeräts statt, welches vom Originalhersteller autorisiert ist und über den öffentlichen Schlüssel des Herstellers verfügt.

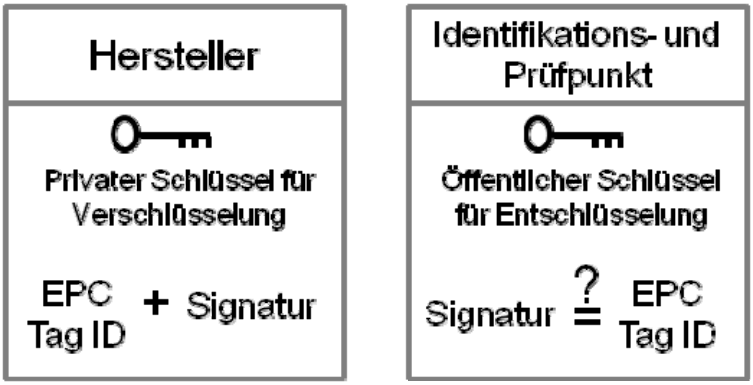

Abbildung 2: Erzeugen eines Originaltransponders beim Hersteller und Prüfung an jedem Identifikations- und Prüfpunkt

Bei Maschinen- und Anlagenteilen ist die Feststellung der Originalität im eingebauten Zustand oder im Moment des Einbaus in die Maschine von besonderer Bedeutung. Spätestens zu diesem Zeitpunkt muss der Kunde sichergehen, dass er nicht fälschlicherweise eine Kopie verwendet. Damit befindet sich der wichtigste Identifikations- und Prüfpunkt in der Maschine, die somit mit der entsprechenden Technik zum Lesen des Transponders ausgestattet sein muss.

Entscheidend für die Originalität einer Komponente ist zunächst nicht die lückenlose Rückverfolgbarkeit durch die logistische Kette oder der Datenbankeintrag beim Hersteller, sondern die Markierung des Bauteils mit einem kopiersicheren Merkmal, einem kryptographisch signierten RFID-Transponder. Eine Aussage über die Produktintegrität, also die bestimmungsgemäße Verwendung und damit die Unversehrtheit des Produkts, ist damit natürlich noch nicht getroffen. Der Kunde kann also insofern getäuscht worden sein, dass er ein gebrauchtes, für einen anderen Markt bestimmtes oder ein gestohlenes Bauteil erworben hat.

2.2 Dokumentation der Prüfergebnisse

Um die Erkenntnisse aus den Originalitätsprüfungen der Identifikations- und Prüfpunkte entlang der Supply Chain und v.a. auch innerhalb der Maschinen beim Kunden nicht verpuffen zu lassen, werden die Prüfergebnisse als einzelne Datensätze gespeichert. So ist im Anschluss eine gezielte Auswertung, u.a. bezüglich der angesprochenen Produktintegrität möglich.

Durch die modulare Struktur des Systems können an beliebigen Punkten der logistischen Kette und integriert in Maschinen Identifikations- und Prüfpunkte aufgebaut werden (siehe Abbildung 3). Dort werden die Prüfinformationen jeweils erzeugt und können lokal gespeichert und genutzt werden. In der Maschine entsteht

so z.B. eine Log-Datei, in der alle Datensätze gespeichert werden und die so Angaben über die Maschinenkonfiguration über die Zeit enthält.

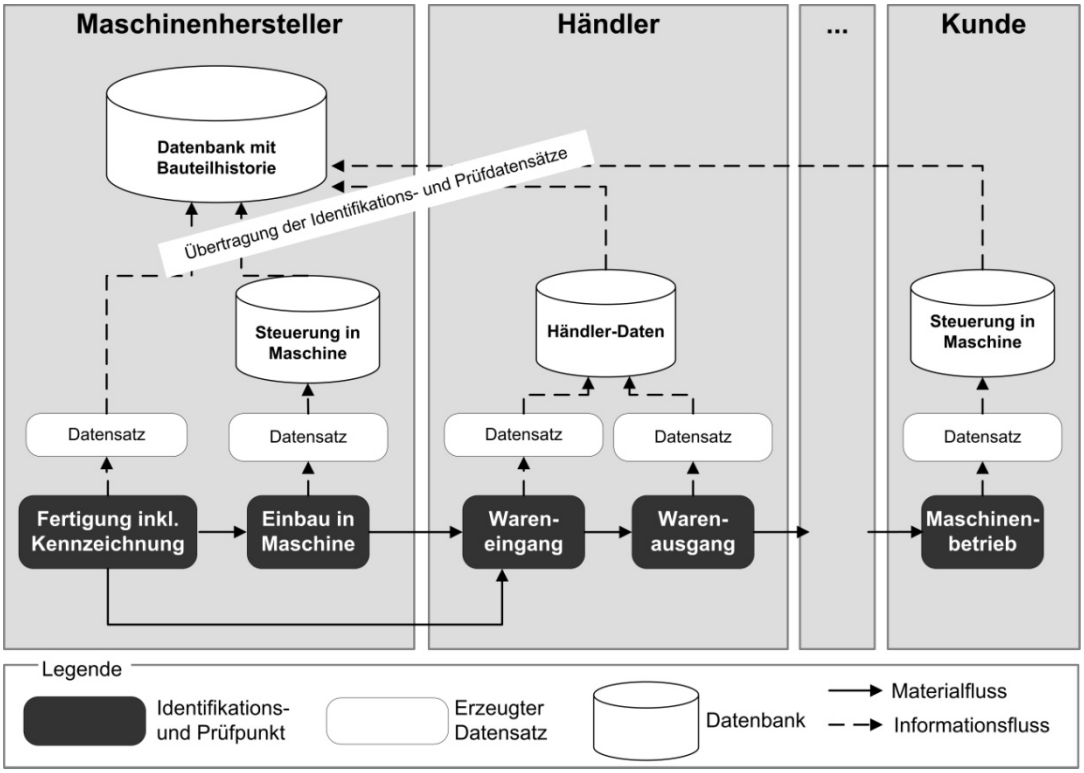

Abbildung 3: Beispiel für Identifikations- und Prüfpunkte entlang der Supply Chain

Gleichzeitig überträgt jeder Identifikations- und Prüfpunkt die Datensätze, bestehend aus der Identifikationsnummer des Bauteils, der Aussage über die Originalität, der Zeit und dem Ort sowie Angaben zum Lesegerät, Prüfer etc., auf den zentralen Server beim Maschinenhersteller (siehe Tabelle 1).

Tabelle 1: Struktur eines Datensatzes

	Name	Bemerkung
Was?	Elektronischer Produktcode (EPC)	Dieser erlaubt es, Objekte mit einer eindeutigen Nummer zu kennzeichnen und beinhaltet - Herstellercode - Sachnummer - Seriennummer (optional)
Original?	Originalität	Aussage über die Originalitätsprüfung des Objekts: echt, nicht echt
	Kennzeichnungstechnologie	Geprüftes Merkmal
Wann?	Zeitpunkt der Lesung	Zeitpunkt der Erfassung des Objektes
Wo?	Identifikations- und Prüfpunkt	Eindeutige Angabe über den Ort
	Maschinennummer	Eindeutige Maschinennummer, sofern sich der Identifikations- und Prüfpunkt in einer Maschine befindet
	Reader-ID	Identifikationsnummer des Lesegeräts, Kennung des Prüfers

Damit das Piraterieschutzsystem zukunftsfähig ist und möglichst vielfältig eingesetzt werden kann, wurde ein Prüfdatenformat entwickelt, welches auf dem EPC-Standard der GS1 [EPC07], [EPC08] beruht. So fügt sich die Entwicklung optimal in bestehende Systeme (z.B. EPC-IS-Anwendungen) ein und die Daten sind problemlos für die Logistik nutzbar. Tracking&Tracing-Informationen und konkrete Daten zur Originalität von Produkten können auf diese Weise in einem System geführt werden, was die ganzheitliche Betrachtung der logistischen Kette unterstützt.
Die Verwendung einer einheitlichen Nummernsystematik gestattet es, die Informationen aus unterschiedlichen IT-Systemen miteinander zu verknüpfen. So wird es möglich, Kunden-, Maschinen- und Komponentendaten (inkl. der Originalitätsaussage) in einer sogenannten Maschinenakte zusammenzuführen. Es entsteht *eine* Sicht auf alle (Prüf-)Daten entlang der Supply Chain, die selbstredend für unterschiedliche Nutzergruppen (z.B. Kunden, Händler, Hersteller) angepasst werden kann und muss.

2.3 Auswertung der gespeicherten Daten und Reaktion

Kunden, Hersteller und Händler können jederzeit Abfragen an die Datenbank stellen und sich über die Historie ihrer Produkte und Komponenten umfassend informieren, was vielfältige Möglichkeiten eröffnet, um effektiv und nachhaltig gegen Produktpiraterie vorzugehen und gleichzeitig alle Vorteile des Tracking & Tracing mit sich bringt.

Für den Hersteller sind v.a. die Prüfergebnisse wichtig, die aussagen, ob die in Maschinen beim Kunden eingebauten Komponenten und Ersatzteile original sind. Denn er leistet Service und Garantie für diese Maschinen. Auf Basis der Datenbankeinträge ist es ihm nun möglich, eine Klassifikation seiner Kunden durchzuführen, kritische Kunden, die bewusst Kopien einsetzen, aber auch treue Kunden zu identifizieren und kritische Maschinen zu erkennen. Die Vertriebs- oder Serviceabteilung kann dann reagieren und aktiv Kontakt zum Kunden aufnehmen, die Motive im direkten Gespräch ermitteln und dem Problem Produktpiraterie frühzeitig entgegentreten. Ein gezieltes Anbieten von Services wie eine erweiterte Garantie, 24h-Service oder Bonusprogramme unter der Voraussetzung der Verwendung von Originalbauteilen sind nur einige Beispiele für effektive Maßnahmen zur Kundenbindung, die einfach zu gestalten sind, wenn der Einsatz originaler Komponenten von beiden Seiten – Herstellern und Kunden – vertrauenswürdig nachvollzogen werden kann.

2.4 Unmittelbare Reaktion auf Prüfergebnisse

Auch unmittelbar nach der Originalitätsprüfung können Reaktionen erfolgen, die ebenfalls geeignet sind, Produktpiraterie einzudämmen. Entscheidend und von großem Nutzen ist die sofortige Rückmeldung an den Prüfer über die Originalität des Bauteils am jeweiligen Identifikations- und Prüfpunkt. Das Prüfergebnis des RFID-

Readers muss also entsprechend visualisiert werden, damit die Information sofort verfügbar ist und v.a. auf Kopien entsprechend reagiert werden kann.

Am Identifikations- und Prüfpunkt in der Maschine können die Daten noch für weitere Funktionen genutzt werden, die den Funktionsumfang der Maschine erhöhen und diese damit für den Kunden attraktiver machen. Sobald das Bauteil als Individuum erkennbar ist, kann diese Information genutzt werden, um einen Verwechslungsschutz bei Werkzeugen umzusetzen, der verhindert, dass ein falsches Werkzeug für die Bearbeitung eingesetzt wird. In Ergänzung können relevante Bauteil- oder Werkzeugdaten sicher und automatisch in die Maschinensteuerung übertragen werden, wenn diese auf dem RFID-Transponder des Bauteils gespeichert oder über die eindeutige Identifikationsnummer verknüpft sind. Für jede Maschine wird sich ein derartiger Zusatznutzen finden lassen, der basierend auf der automatischen und eindeutigen Identifikation einzelner Ersatzteile und Komponenten umfassenden Mehrwert für den Kunden erzeugt. Im Sinne des Produktpirateriesschutzes sind diese Funktionalitäten nur mit dem jeweiligen Sicherheitsmerkmal der Originalkomponenten umsetzbar, um den Know-how-Vorsprung des Maschinenherstellers zu schützen.

3 Ausweitung auf weitere sichere Kennzeichnungstechnologien

Wie dargestellt bietet die RFID-Technologie große Potenziale, um Bauteile und Komponenten im Maschinen- und Anlagenbau vor Produktpiraterie zu schützen. Im Wesentlichen beruht diese Fähigkeit auf der Fälschungssicherheit und Eindeutigkeit der Markierung. Aus diesem Grund sind neben der RFID-Technologie weitere Kennzeichnungstechnologien geeignet, die diese Eigenschaften aufweisen. Sie müssen eine eindeutige Aussage über die Originalität zulassen und das Bauteil individualisieren. Für die Manipulationssicherheit gilt das Gleiche wie bei RFID: nur die sichere Applikation des Merkmals auf dem Bauteil führt zu einem sicheren Schutzsystem.

Eine umfassende Recherche verfügbarer Kennzeichnungstechnologien ergab eine konsolidierte Liste von 22 Technologien, die für die Anwendung im Maschinen- und Anlagenbau grundsätzlich geeignet erscheinen. Dies bedeutet nicht, dass diese für jedes Unternehmen und jedes zu schützende Bauteil zu empfehlen sind. Es gilt die Anforderungen für einen bestimmten Anwendungsfall, d.h. eine betrachtete Komponente, genau zu analysieren und dann zu entscheiden, welche Kennzeichnungstechnologie diese optimal erfüllt. Ein im Rahmen des Forschungsprojekts ProAuthent entwickelter Leitfaden unterstützt die Auswahl anhand technischer und betriebswirtschaftlicher Einflussgrößen.

Durch das in Abschnitt 2.2 vorgestellte standardisierte Prüfdatenformat können Lese- oder Prüfgeräte beliebiger Kennzeichnungstechnologien angebunden und die resultierenden Daten vom Datenbanksystem verarbeitet werden. Damit das Prüfen der Komponenten möglichst komfortabel und aufwandsarm geschehen kann, bieten

sich automatische Prüfprozesse an. Vor allem für günstige Bauteile kann jedoch auch eine manuelle Prüfvariante sinnvoll sein. Das implementierte IT-System bietet deshalb sowohl Schnittstellen für die Anbindung von Lesegeräten als auch eine Eingabemaske über die Ergebnisse manueller Prüfungen gespeichert werden. Die Qualität der vom Menschen erzeugten Ergebnisse hängt hierbei natürlich von der Qualifikation der prüfenden Person ab.

Um die Wertigkeit der gespeicherten Prüfergebnisse möglichst gut einschätzen zu können, enthält jeder Datensatz die Kennzeichnungstechnologie, die zur Prüfung herangezogen wurde, und die ID des Prüfgeräts bzw. den Namen des Prüfers bei manuellen Einträgen.

Exemplarisch wurden die folgenden vier Kennzeichnungstechnologien in einem Demonstrationssystem integriert: Copy Detection Pattern (optisches Rauschmuster), IR-Farbpigmente, Hologramme sowie passive RFID-Transponder. Dabei wird außer bei den Hologrammen automatisch geprüft. Die resultierenden Datensätze werden lokal gespeichert, über eine gesicherte Verbindung in eine zentrale Datenbank übertragen und dort ausgewertet.

4 Pilotinstallationen

Die im Forschungsprojekt beteiligten Unternehmen aus dem Maschinen- und Anlagenbau sind an der Entwicklung des Systems aktiv beteiligt und unterstützen die Validierung des Systems durch konkrete Pilotinstallationen in ihren Unternehmen und ihren Maschinen.

Im Laufe des Projekts haben die Firmen auf Basis einer umfassenden Analyse der Risikosituation ermittelt, welche Bauteile vorrangig durch eine Kennzeichnung vor Produktpiraterie zu schützen sind. Im Anschluss galt es passende Kennzeichnungstechnologien auszuwählen, wozu alle aus dem jeweiligen Anwendungsfall resultierenden Anforderungen ermittelt werden mussten. In den Pilotinstallationen kommen nun ebenfalls die bereits im Demonstratorsystem umgesetzten vier verschiedenen Kennzeichnungstechnologien zum Einsatz, die konkrete, von Produktpiraterie bedrohte Komponenten schützen sollen. Der Fokus der Pilotinstallationen liegt auf dem Aufbau eines Identifikations- und Prüfpunktes, der vollständig in die entsprechenden Maschinen integriert ist. Bei jedem der drei Unternehmen ist sowohl eine sofortige Reaktion auf die Originalitätsprüfung über die Steuerung der Maschine (Warnhinweis, Verwechslungsschutz etc.) als auch die Auswertung der gesammelten Daten in den betrieblichen Informationssystemen geplant. So werden zum Ende des Forschungsprojekts vier realisierte Systeme anschaulich die Funktionen und Möglichkeiten des entwickelten Pirateriesschutzsystems aufzeigen können.

5 Zusammenfassung

Im vorgestellten Schutzsystem zur Abwehr von Produktpiraterie ist es gelungen, Originalitätsmarkierungen und Tracking&Tracing-Ansätze effektiv zu verknüpfen. So ist es einfach und sicher möglich, Kopien zu entdecken und kritische Bauteile in Maschinen und Anlagen vor Produktpiraterie zu bewahren. Durch die Speicherung der Prüfdaten in einer zentralen Datenbank sind außerdem umfassende Zusatznutzen realisierbar, die für die Kunden neue Dienstleistungen und eine vereinfachte Kommunikation mit dem Hersteller mit sich bringen und die Maschinenhersteller in ihrer Service- und Vertriebsarbeit unterstützen. Dies führt zur wichtigen Kundenbindung, die den Erfolg des Systems langfristig sicherstellen kann. Denn ein Markt, in dem Hersteller und Kunden kooperativ zusammenarbeiten, ist wohl die größte Hürde für Produktpiraten.

Literatur

[BMB10] Bundesministerium für Bildung und Forschung: Forschungsoffensive gegen Produktpiraterie. http://www.bmbf.de/de/12095.php: August 2010.

[EPC07] GS1 EPCglobal: EPC Information Services (EPCIS) Version 1.0.1 Specification, Errata Approved by TSC on September 21, 2007.

[EPC08] GS1 EPCglobal: EPCglobal Tag Data Standard Version 1.4, Ratified on June 11, 2008.

[GS08] GS1 Germany: Fälschungssicherheit – Wirksame Konzepte zum Schutz von Marke und Verbraucher. Köln: GS1 Germany, 2008.

[GS10] GS1 Germany: Tracking & Tracing – GS1-Standards sorgen für Transparenz. Köln: GS1 Germany, 2010.

[ICC06] ICC Counterfeiting Intelligence Bureau: anti-Counterfeitign Technology – A Guide to Protecting and Authenticating Products and Documents. ICC Publication No 630: 2006.

[RGO08] Reinecke, M.; Gärtner, H.; Overmeyer, L.: Schutzkonzepte gegen Produktpiraterie in der Pharmaindustrie. In: Industrie Management 6/2008.

[VDM08] VDMA: Untersuchung zur Produkt- und Markenpiraterie. Frankfurt: VDMA, 2008.

[WAB+07] Wildemann, H; Ann, C.; Broy, M; Günthner, W.; Lindemann, U.: Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie. München: TCW, 2007.