Technische Universität München

Fakultät für Maschinenwesen

fml – Lehrstuhl für Fördertechnik Materialfluss Logistik

Schutz vor Produktpiraterie durch Kennzeichnung und Authentifizierung von Komponenten und Ersatzteilen im Maschinen- und Anlagenbau

Dipl.-Wi.-Ing. Dominik Simon Stockenberger

Vollständiger Abdruck der von der Fakultät für Maschinenwesen der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender:

Univ.-Prof. Dr.-Ing. Udo Lindemann

Prüfer der Dissertation:

1. Univ.-Prof. Dr.-Ing. Dipl-Wi.-Ing. Willibald A. Günthner
2. Univ.-Prof. Dr. Dr. h. c. mult. Horst Wildemann

Die Dissertation wurde am 21.01.2014 bei der Technischen Universität München eingereicht und durch die Fakultät für Maschinenwesen am 14.05.2014 angenommen.

Dominik Simon Stockenberger

Schutz vor Produktpiraterie durch Kennzeichnung und Authentifizierung von Komponenten und Ersatzteilen im Maschinen- und Anlagenbau

fml – Lehrstuhl für Fördertechnik Materialfluss Logistik
Prof. Dr.-Ing. Dipl.-Wi.-Ing. Willibald A. Günthner
Technische Universität München

Herausgegeben von:
Prof. Dr.-Ing. Dipl.-Wi.-Ing. Willibald A. Günthner
fml – Lehrstuhl für Fördertechnik Materialfluss Logistik
Technische Universität München

Zugleich:
Dissertation. München: Technische Universität München, 2013

ISBN: 978-3-941702-39-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Layout und Satz: Dominik Stockenberger

Printed in Germany 2013

Investition in Wissen bringt die höchsten Zinsen.

Benjamin Franklin

Wer durch Betrug Gelingen erlangt, dessen Erfolg ist nicht von Dauer
und seine Siege verwandeln sich in Niederlagen.

Lü Bu We

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am fml – Lehrstuhl für Fördertechnik Materialfluss Logistik der Technischen Universität München und basiert auf meiner Arbeit im Projekt „ProAuthent – Integrierter Produktpirateriеschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau“. Für die finanzielle Förderung dieses Forschungsvorhabens möchte ich mich beim Bundesministerium für Bildung und Forschung bedanken.

Mein besonderer Dank gilt Herrn Prof. Dr. Willibald A. Günthner, der mir an seinem Lehrstuhl nicht nur die Promotion, sondern auch eine abwechslungsreiche und interessante Arbeit mit vielen Projekten in Forschung und Industrie verknüpft mit vielen, auch internationalen, Konferenzen ermöglichte. Weiterhin danke ich Herrn Univ.-Prof. Dr. Dr. h. c. mult. Horst Wildemann für die Übernahme des Koreferats und dem Interesse an meiner Arbeit sowie Herrn Univ.-Prof. Dr.-Ing. Udo Lindemann für die Übernahme des Vorsitzes der Prüfungskommission.

Auch gilt mein Dank allen Kolleginnen und Kollegen am Lehrstuhl für die jederzeit angenehme, äußerst freundschaftliche und stets wertschätzende Atmosphäre, die sehr zum freien Denken und kreativem Arbeiten anregt. Besonders hervorheben möchte ich Frau Janina Durchholz, die gemeinsam mit mir das Forschungsprojekt ProAuthent sehr erfolgreich bearbeitet und mich bei der Erstellung meiner Dissertation immer mit sehr guten Ratschlägen unterstützt hat. Zudem bedanke ich mich bei meinem Gruppenleiter Herrn Stefan Galka und den Mitarbeitern/innen der Arbeitsgruppe „RFID“. Nicht zuletzt danke ich auch allen Angestellten des Lehrstuhls, die mir bei allen kleineren und größeren Problemen stets hilfreich zur Seite standen, insbesondere Herrn Tobias Hemmauer und der gesamten Werkstatt.

Weiters gilt mein Dank allen Forschungs- und Industriepartnern, die im Forschungsprojekt ProAuthent zum Gelingen der Forschungsarbeit beigetragen und stets kritisch-konstruktiv mitgearbeitet haben:

- Homag Group AG, Schopfloch
- Infoman AG, Stuttgart
- Müller Martini GmbH, Ostfildern-Kemnat

- Multivac Sepp Haggenmüller GmbH & Co. KG, Wolfertschwenden
- Schreiner Group GmbH & Co. KG., Oberschleißheim
- Vollmer Werke Maschinenfabrik GmbH, Biberach / Riß
- Lehrstuhl für Betriebswirtschaft, Unternehmensführung, Logistik und Produktion, Univ.-Prof. Dr. Dr. h. c. mult. Horst Wildemann, Technische Universität München
- Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum, Prof. Dr. jur. Christoph Ann, LL.M. (Duke Univ.), Technische Universität München

Dabei möchte ich im Besonderen den Projektleitern/-innen und -mitarbeitern/-innen bei den Projektpartnern namentlich danken: Ulrich Doll, Dr. Manuel Görtz, Jürgen Bender, Gunnar Kurz, Dr. Birte Schmidt-Riediger, Dr. Kai Schnapauff, Thomas Völcker, Wolfgang Miller, Wolfgang Schlaucher, Patrick Pommer, Tilman Tschöke, Dr. Ronny Hauck.

Bei der Erstumsetzung der Forschungsinhalte in einem Testdemonstrator haben viele Studenten mitgewirkt. Besonders bedanken möchte ich mich dabei bei Christoph Brosda, Marco Dewitz, Dieter Hahn und Eduard Malakov. Zudem bedanke ich mich bei allen Korrekturlesern, insbesondere bei Janina Durchholz, Stefan Galka, Dr. Manuel Görtz, Daniela Petruschke und Ulrich Stockenberger für ihre Arbeit und stets offene und konstruktive Kritik.

Bedanken möchte ich mich auch bei meinen Eltern Rita und Josef Stockenberger für die Unterstützung und Förderung während meines ganzen bisherigen Lebenswegs. Mein besonderer Dank gilt meiner Partnerin Daniela für ihre liebevolle und dauerhafte Unterstützung während der Erarbeitung der vorliegenden Arbeit und insbesondere für ihre große Geduld. Danke!

Aus Gründen der besseren Lesbarkeit wird in der vorliegenden Arbeit fortan auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Garching b. München im November 2013,
Dominik Stockenberger

Kontakt: produktpirateriesschutz@outlook.com

Kurzzusammenfassung

Produktpiraterie verursacht jährlich weltweit wirtschaftliche Schäden in Milliardenhöhe, bedroht den Erfolg vieler Originalhersteller und bringt diese um die Rendite ihrer Investitionen in Forschung und Entwicklung. Dabei sind im Maschinen- und Anlagenbau insbesondere die hoch profitablen Ersatzteile und Maschinenkomponenten betroffen. Juristische Maßnahmen bilden das Fundament für den Kampf gegen Produktpiraterie, greifen aber zu kurz und entfalten ihre Wirkung meist erst, wenn der Schaden bereits eingetreten ist. Gerade bei den international arbeitenden Unternehmen des Maschinen- und Anlagenbaus braucht es daher neben den juristischen noch weitere Maßnahmen, um dem Problem der Produkt- und Markenpiraterie Herr zu werden.

Bei den Unternehmen gilt der Einsatz von Sicherheitstechnologien am erfolgversprechendsten. Deren Einsatz ist jedoch im Maschinen- und Anlagenbau gering ausgeprägt. Gründe dafür sind, dass viele Unternehmen die technischen Möglichkeiten für ungeeignet halten oder erst gar nicht kennen. Daraus lässt sich ableiten, dass in diesem Bereich breiter Nachholbedarf vorhanden ist. In der vorliegenden Arbeit wird daher erarbeitet, welche technischen Möglichkeiten im Bereich von Sicherheitsmerkmalen existieren.

Ausgehend von einem umfassenden strukturierten Katalog mit verfügbaren Sicherheitsmerkmalen wird ein strategisches Vorgehen entwickelt, das schrittweise aufzeigt, wie Sicherheitsmerkmale ausgewählt und zur Kennzeichnung und Authentifizierung von Komponenten und Ersatzteilen verwendet werden können. Dabei werden für die Unternehmen Methoden ausgearbeitet, um die folgenden Schritte einfach, strukturiert und zielführend bewältigen zu können:

- Identifikation schützenswerter Komponenten und Ersatzteile
- Auswahl passender Kennzeichnungs- und Authentifizierungstechnologien auf Basis technischer sowie wirtschaftlicher Kriterien
- Hinweise für eine erfolgreiche Integration der ausgewählten Sicherheitsmerkmale in Komponenten und Ersatzteilen
- Konzeption und Struktur eines umfassenden IT-Systems für den Produktpirateriesschutz zur Einbindung der ausgewählten Sicherheitsmerkmale

- Implementierung geeigneter Systemreaktionen und Integration passender Zusatznutzen zur Erzeugung einer Win-win-Situation

Ziel ist die Errichtung eines ganzheitlichen Produktpiraterie-Schutzsystems zum Schutz

- der Kunden, welche sicher sein können, Originalwaren einzusetzen,
- der Originalmaschinen, die eigenständig den Einsatz von Originalteilen bestätigen,
- der Hersteller, die eigene Originalbauteile zweifelsfrei und sicher von Kopien unterscheiden, und
- aller Beteiligten im Wertschöpfungs- und Logistiknetzwerk, welche die Originalwaren leicht erkennen und authentifizieren können.

Da passende Maßnahmen gegen Produkt- und Markenpiraterie stets individuell und für den spezifischen Einzelfall entwickelt und implementiert werden müssen, ermöglicht die vorliegende Arbeit den Unternehmen durch die entwickelten Methoden das selbständige Erarbeiten passender Lösungen für die eigenen Maschinen und deren Komponenten und Ersatzteile. Neben der methodisch gestützten Bestimmung schützenswerter Bauteile sowie passender Sicherheitsmerkmale ermöglicht der modulare Aufbau des ganzheitlichen Produktpiraterie-Schutzsystems auch eine unternehmensindividuelle Anpassung und Implementierung inklusive ausgewählter Systemreaktionen und Zusatznutzen.

Abstract

Product piracy causes worldwide economic damage of the order of a billion. Moreover, it poses a serious threat for the success of original manufacturers and their return on investment in research and development. In the sector of mechanical engineering it is predominantly the highly profitable spare parts and components which are affected. Legal measures serve as a basis for the fight against product piracy. These measures, however, are mostly insufficient and only take effect after the cause of damage. For this reason, further measures by mechanical engineering companies acting internationally to master product piracy effectively are required.

Companies regard the use of safety features and technologies as the most promising method. They are, however, not very often made use of in the mechanical engineering sector. This is due to the fact that many companies do either consider these features to be inappropriate or they are not very familiar with them. As a consequence, additional requirements seem to be necessary in this sector.

This thesis therefore presents technical possibilities in the area of safety features and suggests how these features can be used in a holistic technical system of marking and authenticating components and spare parts to protect these parts from product piracy. Moreover, strategic procedure based on an extensively structured catalogue of existing security features developed to construct a holistic technical system using fraud resistant security features will be suggested. To be able to carry out the following steps in an easy, structured and purposeful manner, methods will be provided:

- identification of critical components and spare parts worth being protected,
- selection of suitable marking in the use of technical and economical criteria for the authentication of the original components and spare parts,
- advice in terms of the successful integration of the chosen security marking into components and spare parts,
- concept and structure of a holistic IT-system to integrate the selected security features in the process of protection from product piracy,
- implementation of suitable reactions and appropriate additional benefits to attain a win-win-situation.

The aim is to create an integrated system to prevent product piracy and to make sure

- customers use the original parts,
- original machines automatically confirming the use of original mounted parts and components are being protected,
- original manufacturers who are able to distinguish between original parts and copies are being protected and
- all people being part of the value-added and supply chain network who identify and authenticate original parts easily are being protected.

Adequate measures against product and product piracy are always individual. They have to be developed and implemented in each case separately. This thesis allows affected companies to independently work out suitable solutions for their machines and for the parts and components by harking back to the developed methods. Besides the methodical identification of critical parts and suitable security features, the modular composition of the holistic anti-counterfeiting system guarantees individual adjustment and implementation for the companies including selected reactions of the system and additional benefits.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
ATA	Air Transport Association (Dachverband amerikanischer Fluggesellschaften)
B2B	Business-to-Business (Geschäftsbeziehungen zwischen mindestens zwei Unternehmen)
BDE	Betriebsdatenerfassung
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMYK	Cyan, Magenta, Yellow, Key (Cyan-Magenta-Gelb-Schwarz-Farbpalette)
ConImit	Bezeichnung eines Forschungsprojekts
EAN	Euroäischen Artikelnummer
EANCOM	Subset von EDIFACT-Nachrichten für den Logistikbereich, Kunstwort aus EAN und Communication [Hom-06]
EASA	European Aviation Safety Agency (Europäsche Agentur für Flugsicherheit)
EBIT	Earnings Before Interest and Taxes (operatives Ergebnis als „Gewinn vor Zinsen und Steuern“)
EC	Electronic Cash
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport

EPC	Electronic Product Code (Elektronischer Produktcode)
EPCIS	EPC Information Services
EZB	Europäische Zentralbank
EZ-Pharm	Anwendung elektronischer Echtheitszertifikate an Verpackungen entlang der Pharmaversorgungskette (Forschungsprojekt)
F&E	Forschung und Entwicklung
FAA	Federal Aviation Administration (US-Luftfahrtaufsichtsbehörde)
GATT	General Agreement on Tariffs and Trade
GE	Geldeinheit
Gen-2-Standard	Standard für RFID-UHF-Transponder, beschrieben in „ISO/IEC 18000-63:2013“ ISO18000-63 sowie in „EPCTM RFID Radio-Frequency Identity Protocols. Class-1 Generation-2 UHF RFID. Protocol for Communications at 860 - 960 MHz” EPC-08
GS1	Global Standards One
GSM	Global System of Mobile Communication
GWB	Gesetz gegen Wettbewerbsbeschränkungen
GZS	Gesellschaft für Zahlungssysteme
HF	High Frequency (Hochfrequenz)
HSK	Hohlschaftkegel
I&K-System	Informations- und Kommunikationssystem
IC	Integrierte Schaltung
ICC	International Chamber of Commerce (Internationale Handels-kammer)
ID	Identifikator oder auch Kennung

IHK	Industrie- und Handelskammer
IPK	Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik
IP-Punkt	Identifikations- und Prüfpunkt
I-Punkt	Identifikationspunkt
ISO	Internationale Organisation für Normung
IT	Informationstechnik
KEP	Kurier-, Express- und Paketdienste
KoPiKomp	Konzept zum Piraterieschutz für Komponenten von Investitionsgütern (Forschungsprojekt)
KoPira	Piraterie-Risiko, Strategien und Maßnahmen (Forschungsprojekt)
LAN	Local Area Network (lokales Netzwerk)
LF	Low Frequency (Langwelle)
LSA	Laseroberflächenauthentifizierung
MIC	Machine Identification Code
MIT	Massachusetts Institute of Technology
MobilAuthent	Supply-Chain-übergreifende Services für die fälschungssichere Produkt-Authentifizierung und -verfolgung (Forschungsprojekt)
NATO	North Atlantic Treaty Organization (Organisation des Nordatlantikvertrags)
OCR	Optical Character Recognition (Optische Zeichenerkennung)
OECD	Organisation for Economic Cooperation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
ONS	Object Naming Service

O-PUR	Bezeichnung eines Forschungsprojekts
PC	Personal Computer
PDF	Portable Document Format ((trans-) portables Dokumentenformat)
PIN	Persönliche Identifikationsnummer
PiratPro	Gestaltung von piraterierobusten Produkten und Prozessen (Forschungsprojekt)
POWF	Physical one-way function
ProAuthent	Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau (Forschungsprojekt)
ProdHaftG	Gesetz über die Haftung für fehlerhafte Produkte
ProOriginal	Produkte ganzheitlich schützen – Originale weltweit verkaufen (Forschungsprojekt)
ProProtect	Produktpiraterie verhindern mit Softwareschutz (Forschungsprojekt)
PROTACTIVE	Präventives Schutzkonzept für Investitionsgüter durch einen ganzheitlichen Ansatz aus Organisation, Technologie und Wissensmanagement (Forschungsprojekt)
PUF	Physical unclonebale function
PZN	Pharmazentralnummer
RBAC	Role Based Access Control (rollenbasierte Zugriffskontrolle)
RFID	Radio-frequency Identification (Radiofrequenzidentifikation)
RGB	Rot-Grün-Blau-Farbraum
SGTIN	Serialized Global Trade Item Number
SLG	Schreib-Lesegerät

SSL	Secure Socket Layer-Protokoll
T&T	Tracking&Tracing
TID	Unique Tag-Identifier
TLS	Transport Layer Security-Protokoll
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UHF	Ultra High Frequency (Ultrahochfrequenz)
UII	Unique Item Identifier
UNO	United Nations Organisation
UWG	Gesetz gegen den unlauteren Wettbewerb
VDMA	Verband Deutscher Maschinen- und Anlagenbau
WIPO	World Intellectual Property Organization
WLAN	Wireless LAN
WTO	World Trade Organization
XML	Extensible Markup Language

Verwendete Formelzeichen

Formelzeichen	Einheit	Bedeutung
$CF_{Barwert}$	[GE]	Gegenwartswert des jährlichen Cash-Flow-Verlusts, somit auf die Periode t=0 abgezinster Cash-Flow-Verlust pro Jahr
$CF_{Barwert, Diff}$	[GE]	Differenz des Gegenwartswerts der jährlichen Cash-Flow-Verluste $CF_{Barwert}$ der verglichenen Szenarien
$CF_{statisch}$	[GE]	statischer Cash-Flow-Verlust aufgrund des Gewinnverlusts des Originalherstellers pro Jahr
g	[%]	Gewinnspanne zur Abbildung des Gewinnverlusts als Anteil des Umsatzverlusts
$G_{O,verl}$	[GE]	Gewinnverlust des Originalherstellers pro Jahr
I	[GE]	Invest des Originalherstellers zur Erzeugung von Sicherheitsmerkmalen und zur Einrichtung eines Gesamtsystems (kann über die Perioden fortgeschrieben werden, falls Folgeinvestitionen erwartet werden)
i	[%]	Kapitalkostensatz
K_0	[GE]	Gegenwartswert der jährlichen Verluste der betrachteten Perioden als Summe der $CF_{Barwert}$
$K_{0,S}$	[GE]	Kapitalwert der Investition in ein Sicherheitsmerkmal und Gesamtsystem aufgrund der Verringerung der Schäden durch Produkt- und Markenpiraterie
k_{var}	[GE]	Preis für ein einzelnes Sicherheitsmerkmal
K_{var}	[GE]	stückzahlabhängige variable Kosten zur Ausrüstung der Originalbauteile mit Sicherheitsmerkmalen

Formelzeichen	Einheit	Bedeutung
η_S	[%]	situationsbezogener Wirkungsgrad eines Sicherheitsmerkmals
N_G	[-]	rechnerische Gesamtstückzahl eines Bauteils im After-Sales pro Jahr
N_K	[-]	Anzahl verkaufter Kopien durch redliche oder unredliche Wettbewerber pro Jahr
$N_{K,S}$	[-]	reduzierte Anzahl der durch redliche oder unredliche Wettbewerber verkauften Kopien aufgrund des Einsatzes von Sicherheitsmerkmalen durch den Originalhersteller
N_O	[-]	Anzahl verkaufter Bauteile des Originalherstellers pro Jahr
$N_{O,G}$	[-]	Anzahl der insgesamt durch den Originalhersteller pro Jahr verkauften Bauteile nach Einführung eines Sicherheitsmerkmals
$N_{O,max}$	[-]	maximale Anzahl der aufgrund des Einsatzes von Sicherheitsmerkmalen durch den Originalhersteller zurückzugewinnende Stückzahl pro Jahr
$N_{O,Z}$	[-]	Anzahl der aufgrund des Einsatzes eines Sicherheitsmerkmals zusätzlich verkaufter Bauteile des Originalherstellers
p	[GE]	Verkaufspreis, den der Originalhersteller pro verkauftem Bauteil realisiert
q_{max}	[%]	bezogen auf N_K maximaler Marktanteil, der zurückgewonnen werden könnte, wenn ein Sicherheitsmerkmal inklusive Gesamtsystem eingeführt werden würde

Formelzeichen	Einheit	Bedeutung
r	[%]	Gewichtungsfaktor zur Gewichtung des Restwerts für die Zeitperioden ab t=8
R_0	[GE]	Fortschreibung der Verluste ab Periode t=8 und Gewichtung mit dem Gewichtungsfaktor r
$S_{0,gesamt}$	[GE]	gesamter Produktpirateriesschaden für das betrachtete schützenswerte Bauteil als Barwert in t=0
t	[a]	Zeitperiode
$\hat{t}$	[a]	Zeithorizont: letzte Zeitperiode, welche in der Wirtschaftlichkeitsrechnung direkt und vollständig abgebildet wird
U_G	[GE]	Gesamter Marktumsatz für das schützenswerte Bauteil, bildet den Umsatz des Originalherstellers ohne Schaden ab
U_O	[GE]	Umsatz des Originalherstellers durch Verkauf der schützenswerten Bauteile pro Jahr
$U_{O,verl}$	[GE]	Umsatzverlust des Originalherstellers pro Jahr
$U_{O,Z}$	[GE]	der aufgrund des Einsatzes eines Sicherheitsmerkmals zu erwartende zusätzliche Umsatz pro Jahr

1 Einführung

„Wir brauchen den Schutz geistigen Eigentums. Wenn wir vom kreativen Imperativ sprechen, dann ist es natürlich von allergrößter Bedeutung, dass es uns gelingt, geistige Innovation auch wirklich vor Piraterie zu schützen.“, so Bundeskanzlerin Dr. Angela Merkel in ihrer Rede auf dem Weltwirtschaftsforum am 25. Januar 2006 in Davos [Mer-06].

Bereits Ende der 1960er Jahre wurde die Weltorganisation für geistiges Eigentum (WIPO: World Intellectual Property Organization) als Ergebnis der „verschiedenen Traditionen und Stränge der Internationalisierung des geistigen Eigentums“ gegründet und ist heute ein Teil der Vereinten Nationen. Die WIPO steht weltweit für die „Idee, dass die ursprünglichen Schöpfer von Werken, die gegen Vervielfältigung geschützt sind, ein Recht auf wirtschaftliche Erträge und moralische Rechte genießen“. Trotz dieser Initiative und der permanenten internationalen Bemühungen zur Angleichung dieser Rechte[1] befindet sich die Welt des geistigen Eigentums aufgrund der Globalisierung und Digitalisierung aktuell in einem „Stadium des Suchens und des Übergangs“. [Sie-13a S. 75 f.]

Dass Produktpiraterie für die Weltwirtschaft eine große und stetig wachsende Bedrohung darstellt und gravierende Folgen und Auswirkungen hat, ist bekannt und wird in dieser Arbeit in einem zusammenfassenden Überblick dargestellt. Neben den Rahmenbedingungen internationaler Verträge und Abkommen bzw. der nationalen Gesetzgebung und der darauf basierenden juristischen Maßnahmen existieren auch technische Möglichkeiten, um sich aktiv vor Produktpiraterie zu schützen.

Das Ziel dieser Arbeit ist die Entwicklung und Ausgestaltung eines technischen Produktpiraterie-Schutzsystems mit dem Einsatz von kopiersicheren Kennzeichen in oder auf schützenswerten Komponenten und Ersatzteilen des Maschinen- und Anlagenbaus, um Produktpiraterie präventiv zu begegnen. Redliche oder unredliche Wettbewerber sollen bereits vor dem Kopieren durch die erkennbaren Sicherheitsmerkmale von einem Kopierversuch abgehalten werden oder es soll zumindest das

[1] z. B. Richtlinien der Europäischen Union, GATT: General Agreement on Tariffs and Trade, Gründung der WTO: World Trade Organization, TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights

Original immer und für alle Beteiligten klar von der Kopie unterscheidbar bleiben. In dieser Arbeit wird daher aufgezeigt,

- wie diese schützenswerten Komponenten und Ersatzteile für Maschinen und Anlagen beim Originalhersteller methodisch unterstützt ausgewählt und
- wie für diese schützenswerten Bauteile auf Basis technischer wie auch wirtschaftlicher Kriterien passende Sicherheitsmerkmale bestimmt werden können,
- wie ein technisches System zur Kennzeichnung und Authentifizierung der markierten Bauteile ausgestaltet werden kann und
- wie passende Systemreaktionen einen Mehrwert und insbesondere weitere Systemfunktionen eine Win-win-Situation für alle Wirtschaftsbeteiligten im Wertschöpfungs- und Logistiknetzwerk des Originalherstellers entstehen lassen.

1.1 Ausgangssituation und Problemstellung

1.1.1 Rolle des deutschen Maschinen- und Anlagenbaus in der Welt

Betrachtet man den weltweiten Handel mit Maschinen liegt Deutschland mit einem Anteil von 16,8 % im Jahre 2010 vor Japan und den USA unverändert auf Platz eins [Wie-12 S. 29]. Dabei ist der Maschinen- und Anlagenbau mit einem Umsatz von rund 200 Mrd. Euro und knapp 1 Mio. Mitarbeitern in etwa 6.000 Unternehmen der größte und damit bedeutendste deutsche Industriezweig [Wie-12 S. 6].

Für den deutschen Maschinen- und Anlagenbau sind seine breite Angebotspalette und ausgezeichnete Qualität charakteristisch: „Mit seinen mehr als 20.000 unterschiedlichen Produkten und seinem hohen technischen Niveau steht der deutsche Maschinen- und Anlagenbau an der Weltspitze.“ [BMWi-11 S. 7]

1.1.2 After-Sales im deutschen Maschinen- und Anlagenbau

Neben dem Neumaschinengeschäft erwirtschaftet die Branche einen erheblichen Anteil des Gesamtumsatzes im After-Sales. In der Investitionsgüterindustrie machte das After-Sales-Geschäft im Jahr 2010 einen Umsatzanteil von etwa 27 % aus. Für 2015 werden 40 % prognostiziert [Imp-11 S. 13]. In manchen Unternehmen, die als

Best-Practice dienen, beträgt dieser Anteil heute bereits bis zu 50 % [Vis-12] oder sogar erheblich mehr [Gla-03 S. 19].

Die Ertrags- und Wachstumspotenziale des Maschinen- und Anlagenbaus liegen somit vor allem im After-Sales [Inn-12]. Dieser Geschäftsbereich ist schon heute hoch profitabel: Das operative Ergebnis (EBIT: Earnings Before Interest and Taxes) liegt mit durchschnittlich 12 % und Spitzenwerten bis 25 % weit über der des Neumaschinengeschäfts mit durchschnittlich 4 % [Imp-11 S. 19, Vis-12]. Aus den Zahlen der Studie der *IMPULS Management Consulting GmbH* lässt sich gemäß *Wienholdt* sogar ableiten, dass im Durchschnitt das After-Sales-Geschäft das Geschäft mit Neumaschinen in seinem Beitrag zum Unternehmensgewinn bereits überholt hat [Wie-11 S. 2].

Bei einer Analyse des After-Sales wiederum ist feststellbar, dass der Ersatzteilverkauf einen erheblichen Anteil einnimmt (siehe Abbildung 1-1).

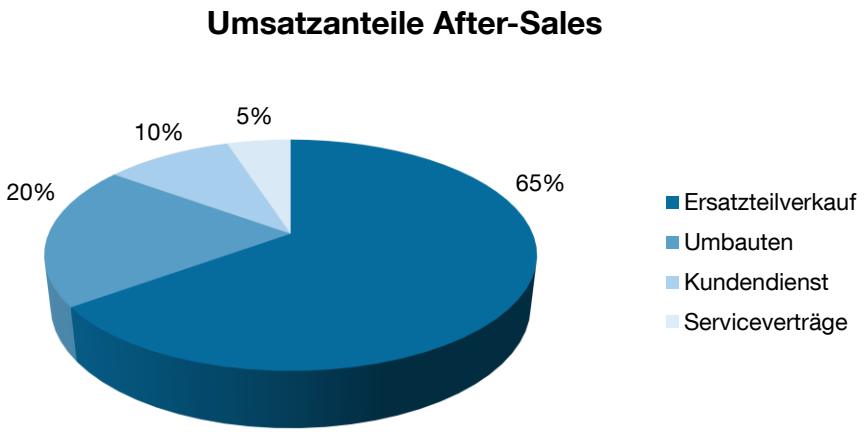


Abbildung 1-1: Umsatzanteile am After-Sales-Service, gemäß Daten aus [Abs-12]

1.1.3 Produkt- und Markenpiraterie weltweit

„Die Produkt- und Markenpiraterie ist eines der größten Wirtschaftsverbrechen unserer Zeit.“, so Rüdiger Stihl, Vorsitzender des Aktionskreises gegen Produkt- und Markenpiraterie [Her-11].

Nach Angaben der aktuellsten Studie der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) könnte der internationale Handel mit Fälschungen und illegal kopierten Produkten im Jahr 2005 ein Volumen von 200 Mrd. US-Dollar erreicht haben [OECD-08 S. 11]. Dies entsprach 2 % des Welthandelsvolumens, das 2005 knapp 10,5 Bio. US-Dollar betrug [WTO-12]. Dabei ist weder der

inländische Handel mit Kopien oder Fälschungen noch das „erhebliche Volumen an raubkopierten digitalen Produkten, die über das Internet vertrieben werden“, beinhaltet [OECD-08 S. 11]. Daher ist davon auszugehen, dass das weltweite Gesamtvolumen der Produkt- und Markenpiraterie mehrere hundert Milliarden US-Dollar mehr beträgt [OECD-08 S. 11].

Statistisch erfasst ist beispielsweise der Wert der vom Zoll sichergestellten Waren. Hierbei ist ein über die Jahre klar aufwärts weisender Trend erkennbar (siehe Abbildung 1-2). Auch die Anzahl der an die OECD berichterstattenden Staaten wächst stetig (siehe Abbildung 1-3). Dies zeigt, dass Produkt- und Markenpiraterie ein weltweit permanent wachsendes Problem ist und als solches erkannt wird.

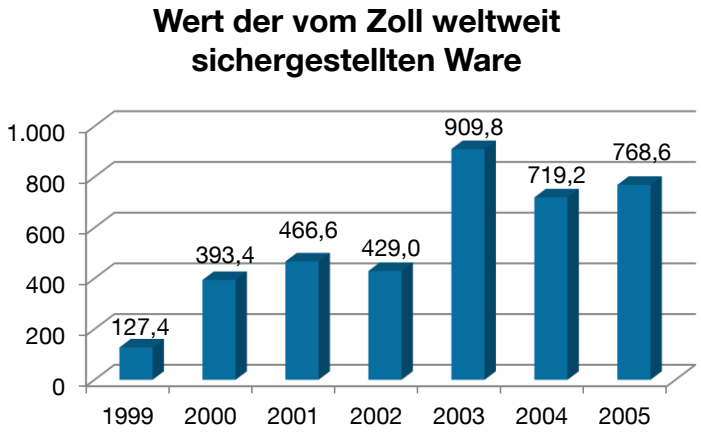


Abbildung 1-2: Wert der vom Zoll weltweit sichergestellten Ware in Mio. US $, gemäß Daten aus [OECD-08 S. 57] [2]

[2] nach Blume geht hier lediglich der Materialwert der beschlagnahmten Güter ein, nicht jedoch deren Marktwert und damit der reale Schaden [Blu-06 S. 74]

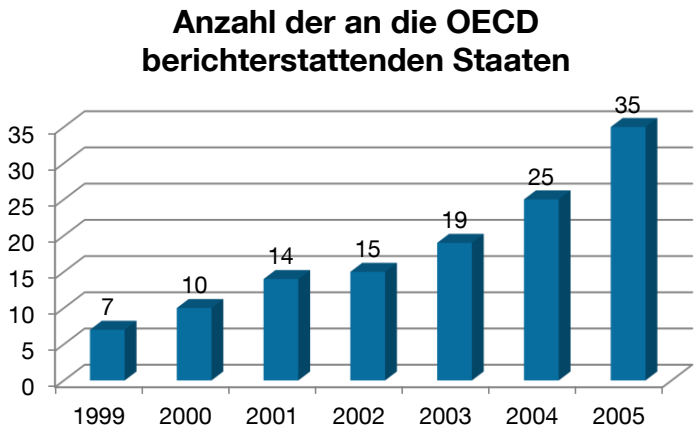


Abbildung 1-3: Anzahl der zu Produkt- und Markenpiraterie an die OECD berichterstattenden Staaten, gemäß Daten aus [OECD-08 S. 57]

1.1.4 Produkt- und Markenpiraterie im deutschen Maschinen- und Anlagenbau

Der weltweite Erfolg des deutschen Maschinen- und Anlagenbaus lockt offenbar Produktpiraten und Kopierer. In den vergangenen Jahrzehnten wurden insbesondere Konsumgüter wie Bekleidung, Accessoires, Taschen, Uhren oder auch Software, Filme und Musik kopiert [Kle-10 S. 7, Fuc-06 S. 18]. Mittlerweile orientieren sich Kopierer um in Richtung anspruchsvoller technischer Produkte wie Autos, Motorräder, Helikopter oder Werkzeugmaschinen [Blu-06 S. 51, S. 56, Fuc-06 S. 19, VDMA-12b]. Dabei sind die qualitativ hochwertigen und weltweit begehrten deutschen Markenprodukte für Kopierer besonders attraktiv [Fuc-06 S. 19].

Der Verband Deutscher Maschinen- und Anlagenbau (VDMA) stellt in einer Umfrage fest, dass 67 % der Maschinen- und Anlagenbauer von Produktpiraterie betroffen sind [VDMA-12a S. 7]. Der Jahresumsatzverlust, der damit verbunden ist, liegt bei 7,9 Mrd. Euro – ein Umsatz dieser Größenordnung entspricht in dieser Branche etwa 7.000 Arbeitsplätzen [VDMA-12a S. 9].

Wie in Abbildung 1-4 erkennbar ist, werden bei 48 % der Unternehmen ganze Maschinen nachgebaut. Insbesondere sind aber bei 52 % der Unternehmen Komponenten und bei 36 % Ersatzteile von Produkt- und Markenpiraterie betroffen.

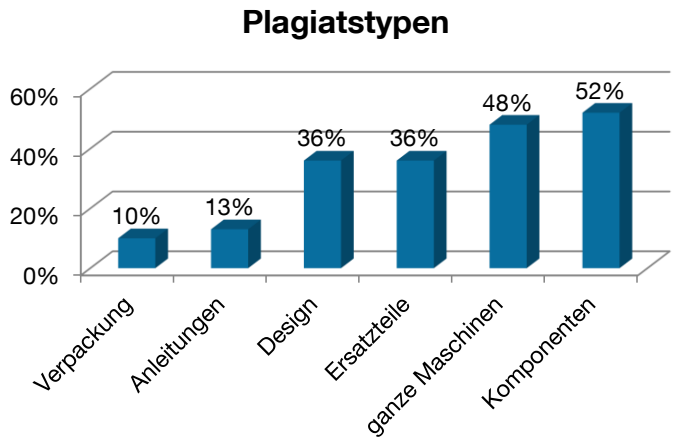


Abbildung 1-4: Plagiatstypen im Jahr 2012, Mehrfachnennung möglich, gemäß Daten aus [VDMA-12a S. 11]

Gerade der Bereich der Ersatzteile und Komponenten, die im After-Sales für die Unternehmen hinsichtlich Umsatz und Gewinn, aber auch hinsichtlich Wachstumschancen so bedeutend sind (siehe Abschnitt 1.1.2), gerät aufgrund dieses Problems stark unter Druck.

1.2 Motivation, Ziel und konzeptioneller Aufbau der Arbeit

1.2.1 Motivation

Das After-Sales-Geschäft erzeugt im deutschen Maschinen- und Anlagenbau bereits heute einen großen Anteil des Umsatzes und des Gewinns. Gleichzeitig ist davon auszugehen, dass dieser Anteil weiter wachsen wird (siehe Abschnitt 1.1.2). Der Verkauf von maschinenspezifischen Komponenten und Ersatzteilen macht am After-Sales-Geschäft etwa 65 % aus (siehe Abbildung 1-1). Gerade hier setzen Produktpiraten an (siehe Abbildung 1-4) und schaden so den Unternehmen massiv.

Mit dem Einsatz technischer Schutzmaßnahmen und ihrem stark präventiven Charakter sowie entsprechender Produktgestaltung könnte eine vorerst unüberwindbare Imitationsbarriere für Produktpiraten erzeugt werden [Hof-10 S. 86]. Der Einsatz technischer Maßnahmen gegen Produktpiraterie ist allerdings im Maschinen- und Anlagenbau mit lediglich 28 % gering ausgeprägt (siehe Abbildung 1-5). Gründe hierfür sind, dass knapp ein Viertel der Unternehmen die am Markt erhältlichen technischen Möglichkeiten für ungeeignet halten, etwa 12 % kennen gar keine geeigneten technischen Schutzmaßnahmen [VDMA-12a S. 18].

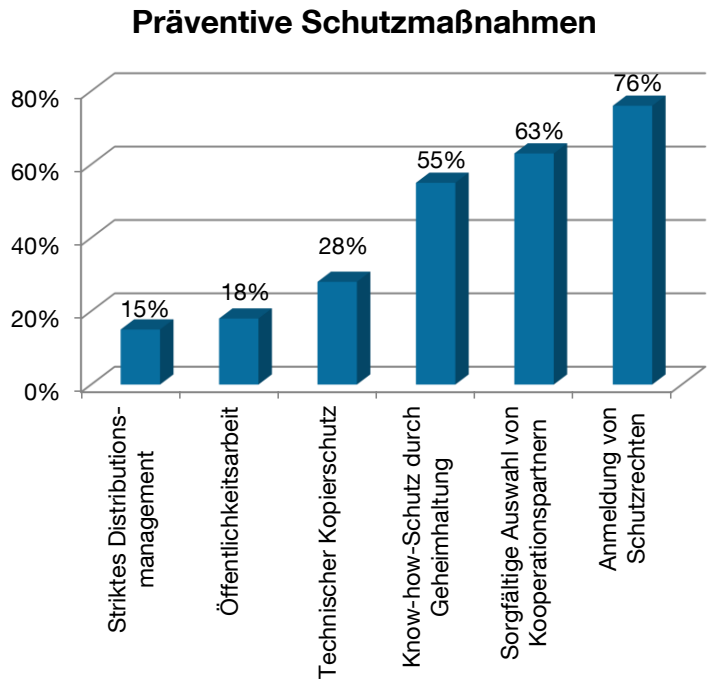


Abbildung 1-5: Einsatz präventiver Schutzmaßnahmen in Unternehmen im Jahr 2012, Mehrfachnennung möglich, gemäß Daten aus [VDMA-12a S. 15]

Demgegenüber steht die Feststellung des Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik (IPK) in Berlin, dass die Unternehmen das größte Lösungspotenzial für den Marken- und Produktschutz im Einsatz von Sicherheitstechnologien sehen (siehe Abbildung 1-6). Auch wird aus der Statistik direkt abgeleitet, dass in diesem Bereich „breiter Nachholbedarf“ existiert. [Krü-06 S. 30]

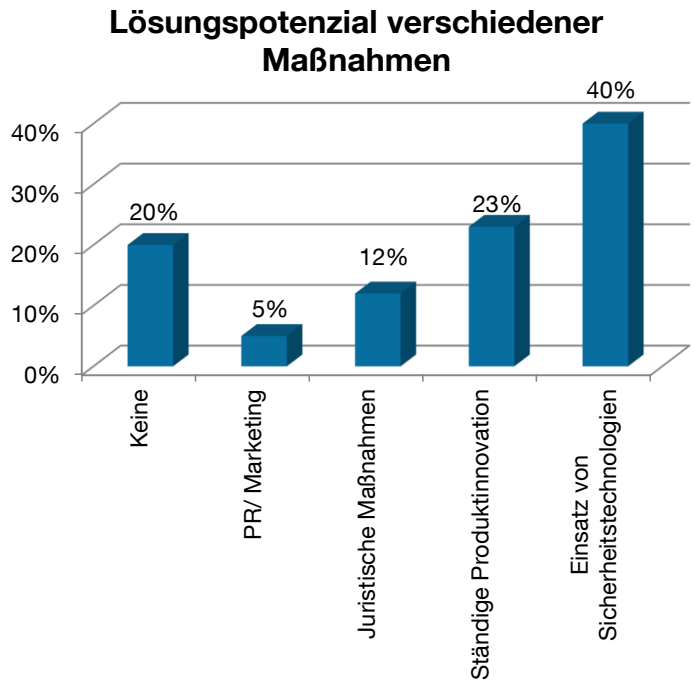


Abbildung 1-6: Lösungspotenzial verschiedener Maßnahmen für den Marken- und Produktschutz, gemäß Daten aus [Krü-06 S. 30]

Die vorliegende Arbeit möchte dazu beitragen, genau diese Lücke zu schließen. Damit verknüpft soll gleichzeitig aufgezeigt werden, wie Originalbauteile während der gesamten Lebensdauer als Originale erkennbar und von Kopien unterscheidbar gemacht werden können. Betrachtet man die Themen Forderungen aufgrund Verfügbarkeitsgarantien, Regressforderungen sowie Produkthaftungsansprüche, müssen in diesen Fällen die beklagten Originalhersteller nachweisen – sofern es so ist –, dass das Bauteil, welches den Schaden verursacht hat, kein Originalbauteil war. In diesen Fällen gilt dieser juristische Grundsatz zur Beweislastverteilung und der Originalhersteller wird sich gegen die erhobenen Forderungen nur dann erfolgreich zur Wehr setzen können, wenn der entsprechende Nachweis gelingt. [Kro-06 S. 19, Gau-12 S. 6, 29]

1.2.2 Zielstellung und Lösungsansatz: Schutz der Kunden, der Maschinen und des Originalherstellers

Das Ziel der vorliegenden Arbeit ist es, Produkt- und Markenpiraterie präventiv zu bekämpfen und nachhaltig zurückzudrängen, um Schäden bei den Maschinen- und Anlagenbauern zu reduzieren oder zu eliminieren, den Wettbewerbsvorteil gegenüber redlichen und insbesondere unredlichen Konkurrenten zu erhalten oder durch neue Maschinenfunktionalitäten sogar auszubauen. Dies soll mit einem technischen

Schutzsystem erreicht werden, das mit kopiersicheren Kennzeichen auf oder in Originalbauteilen arbeitet.

Eine detaillierte Betrachtung dieses Themenkomplexes ermöglicht es, das in Abbildung 1-7 dargestellte kaskadierende Zielsystem zu formulieren, bei dem die Einzelziele systematisch aufeinander aufbauen. Im Ziel 1 wird mittels kopiersicherer Kennzeichen auf oder in Originalbauteilen eine abschreckende Botschaft transportiert, die nach Experteneinschätzung präventiv gegen das Kopieren von Originalbauteilen wirkt [Hof-10 S. 86, Gau-12 S. 24, S. 31 ff., Wil-07 S. XI, S. 9, S. 64]. Die Botschaft lautet, dass der Originalhersteller Maßnahmen ergriffen hat, dass seine Bauteile nicht in allen Details kopierbar sind und dass ein Kopierversuch immer zu einem Ergebnis führt, das für alle Wirtschaftsbeteiligten von Originalbauteilen unterscheidbar ist. Diese permanente Unterscheidbarkeit ist in Ziel 2 formuliert, für den Fall, dass dennoch Kopien erzeugt werden, und bezieht sich ebenfalls auf Graumarktware oder Teile aus der Dritten Schicht (siehe Übersicht in Abbildung 2-2, S. 32).

Ziel 3 gilt dem Schutz des gesamten Wertschöpfungs- und Logistiknetzwerks des Originalherstellers inklusive der Maschinen und Anlagen beim Kunden. Dabei sollen im Netzwerk technisch passend ausgestattete Identifikations- und Prüfpunkte (IP-Punkte) platziert und die Originalität von Komponenten und Ersatzteilen durchgängig geprüft werden. Dies soll insbesondere auch beim Einsatz von Komponenten und Ersatzteilen in einer Maschine oder Anlage möglich sein, die selbsttätig feststellen kann, ob Originale eingesetzt werden. Damit soll kopierten Bauteilen, Bauteilen aus dem Graumarkt oder der Dritten Schicht der Weg in das wirtschaftliche Netzwerk des Originalherstellers versperrt werden.

Das Ziel 4 sieht vor, dass das Prüfergebnis nicht nur kurzfristig im Augenblick der Authentifizierung eines Bauteils der jeweiligen prüfenden Instanz vorliegt, sondern auch im Nachgang jederzeit einsehbar und nachvollziehbar ist. So soll eine neue Transparenz erzeugt werden, um etwaige Auseinandersetzungen im Bereich von Verfügbarkeitsgarantien oder auch Produkthaftungsansprüchen auf Basis objektiver Daten schnell klären zu können. Das Ziel 5 nutzt das technische System aus gekennzeichneten Originalbauteilen und IP-Punkten, um mit neuen Funktionalitäten für alle Wirtschaftsbeteiligten Zusatznutzen zu erzeugen und damit den Wettbewerbsvorteil des Originalherstellers zu erhalten oder sogar auszubauen.

Ziel 1	**Verhinderung des Nachbaus bzw. der Fälschung von Originalkomponenten und -ersatzteilen**
Ziel 2	**Dauerhafte Unterscheidbarkeit zwischen Original und Kopie, Graumarktware oder Bauteilen aus der Dritten Schicht**
Ziel 3	**Schutz des gesamten Wertschöpfungs- und Logistiknetzwerks der Originalhersteller inklusive der Maschinen und Anlagen bei Kunden mit Hilfe technisch passend ausgestatteter Identifikations- und Prüfpunkte**
Ziel 4	**Erzeugung einer neuen Transparenz im Wertschöpfungs- und Logistiknetzwerk inklusive Maschinen und Anlagen durch nachhaltige Dokumentation der Prüfergebnisse**
Ziel 5	**Implementierung neuer Funktionalitäten zum Erhalt oder Ausbau des Wettbewerbsvorteils der Originalhersteller**

Abbildung 1-7: Ziele für das technische Produktpiraterie-Schutzsystem

Zur Erreichung dieser Ziele werden in dieser Arbeit zwei existierende Ansätze zu einem effektiven technischen Schutzsystem kombiniert. Das technische Produktpiraterie-Schutzsystem soll den Ansatz des Produkt- und Markenschutzes, der es ermöglicht, die Originalität von Objekten mittels Sicherheitsmerkmalen zweifelsfrei festzustellen, kombinieren mit dem Ansatz des Tracking&Tracing aus der Logistik, der es ermöglicht, Objekte auf ihrem Weg durch die Supply-Chain zu verfolgen (siehe Abbildung 1-8). Damit soll das gesamte Wertschöpfungs- und Logistiknetzwerk einschließlich der Maschinen und Anlagen bei Kunden vor dem Eindringen und Einsatz von Kopien abgesichert werden. Der Schutz soll sich erstrecken auf und wirken für

- Kunden, welche sicher sein können, Originalwaren einzusetzen,
- Maschinen, die eigenständig den Einsatz von Originalteilen prüfen,
- Hersteller, die eigene Originalbauteile zweifelsfrei und sicher von Kopien unterscheiden, und
- alle Beteiligten im Wertschöpfungs- und Logistiknetzwerk, welche die Originalwaren leicht erkennen und authentifizieren können.

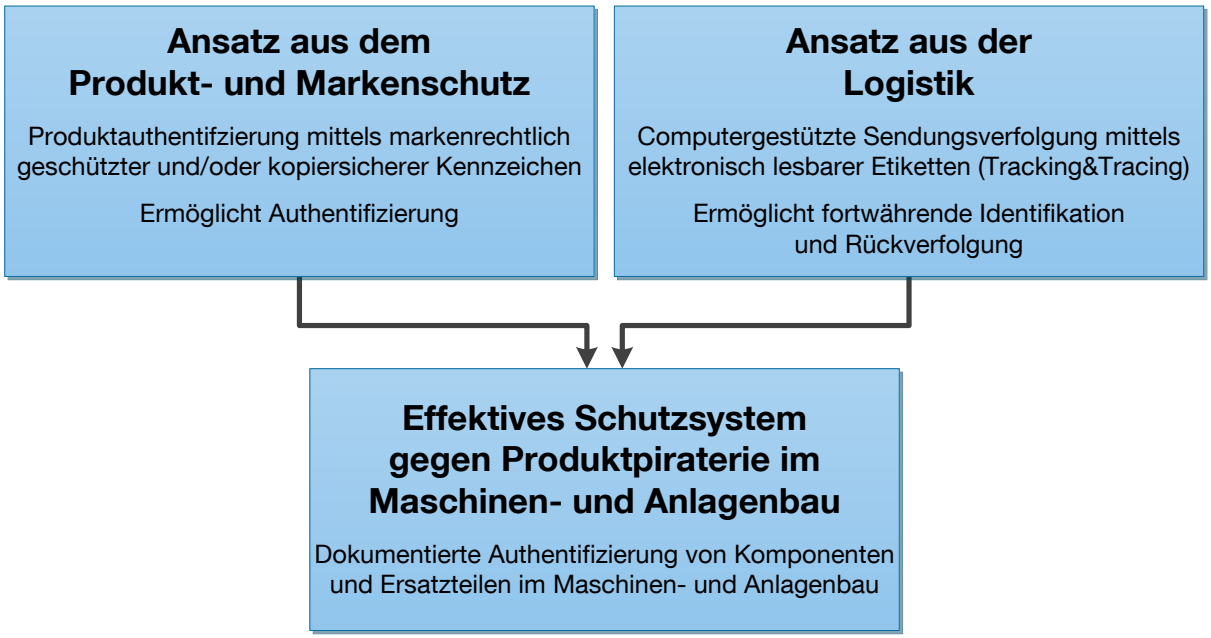


Abbildung 1-8: Logische Verknüpfung existierender Lösungen zu einem Schutzsystem für den Maschinen- und Anlagenbau [3]

1.2.3 Konzeptioneller Aufbau der Arbeit

Die gesamte Arbeit gliedert sich in zehn Kapitel. Die einzelnen Abschnitte der Kapitel bauen dabei inhaltlich aufeinander auf und sind in Abbildung 1-9 und Abbildung 1-10 somit nacheinander angeordnet. Teilweise sind die Unterabschnitte nebenläufig oder speziell bei den Beispielen begleitend zu sehen und damit nebeneinander abgebildet.

In Kapitel eins wird die aufgrund von Produkt- und Markenpiraterie problembehaftete und bedrohliche Lage des deutschen Maschinen- und Anlagenbaus dargestellt. Demgegenüber steht die Feststellung, dass die Unternehmen einen Ausweg im Einsatz von Sicherheitstechnologien sehen, diese aber für das eigene Unternehmen ungeeignet halten oder erst gar nicht kennen. Die vorliegende Arbeit möchte diese Lücke durch wissenschaftlich aufgearbeitete und strukturierte Information sowie technische Lösungen schließen. Abschließend wird das Ziel und der Lösungsansatz für die vorliegende Arbeit vorgestellt, um dem Problem der Produkt- und Markenpiraterie wirksam zu begegnen.

In Kapitel zwei werden als zentrale Begriffe „Produktpiraterie“ und „Markenpiraterie“ definiert. Diese sind, wie alle Definitionen in dieser Arbeit, umrahmt hervorgehoben.

[3] Definition zu Tracking&Tracing aus [Arn-08 S. 596, Hom-06 S. 231]

Desweiteren werden die starken bestehenden Anreize für Produktpiraten sowie die entstehenden Schäden für Hersteller, Verbraucher und die Gesellschaft insgesamt dargestellt. Um Produktpiraterie zu begegnen, haben Unternehmen verschiedene Handlungsmöglichkeiten. Juristische Mittel stellen den häufigsten Ansatz dar, Produktpiraterie zu bekämpfen. Sie werden jedoch nur kurz inklusive ihrer Grenzen erläutert, da dies nicht der Schwerpunkt der vorliegenden Arbeit ist. Die Abgrenzung des für die vorliegende Arbeit geltenden Untersuchungs- und Einsatzbereichs sowie weitere grundlegende Begriffsdefinitionen beschließen das Kapitel.

Kapitel drei und vier widmen sich dem aktuellen Stand der Technik sowie dem aktuellen Stand der Wissenschaft und Forschung. Es werden existierende Sicherheitsmerkmale sowie Systeme zur Nachverfolgung und Sicherstellung der Originalität, aber auch aktuelle oder kürzlich abgeschlossene Forschungsaktivitäten im Themenfeld vorgestellt. Abschließend wird die Forschungslücke aufgezeigt, welche die vorliegende Arbeit schließen möchte.

Als einleitendes Kapitel für die Entwicklung eines Gesamtsystems zur Schließung der aufgezeigten Forschungslücke wird in Kapitel fünf ein Referenzszenario eingeführt. Zudem wird der grundlegende Unterschied zwischen einerseits von Produkt- und Markenpiraterie betroffenen und andererseits schützenswerten Bauteilen fest- und Kriterien zur Bestimmung der schützenswerten Bauteile aufgestellt. Der nächste Abschnitt zeigt dann auf, welches strategische Vorgehen zum Schutz dieser schützenswerten Bauteile sinnvoll ist. Abschließend werden die Anforderungen an Sicherheitsmerkmale sowie das technische Produktpiraterie-Schutzsystem formuliert.

Das Kapitel sechs kann als kurzer Hinweis verstanden werden, dass das Branding von Originalkomponenten und -ersatzteilen aufgrund der eingetragenen gewerblichen Schutzrechte (z. B. eine Marke) ein wesentlicher Schritt für die Kennzeichnung von Originalbauteilen zur Abgrenzung gegenüber Kopien von redlichen oder unredlichen Wettbewerbern darstellt. Da es sich dabei um ein eigenes Themenfeld in der Wissenschaft handelt, werden in Kapitel sechs lediglich Hinweise auf weiterführende Quellen und Beispiele von Realisierungen gegeben.

Die Kapitel sieben, acht und neun sind als eine Einheit zu sehen, in denen das gesamte technische Produktpiraterie-Schutzsystem strukturiert und logisch aufeinander aufgebaut wird.

Kapitel sieben widmet sich vollständig dem Thema Sicherheitsmerkmale sowie der Kennzeichnung schützenswerter Bauteile. Zunächst erfolgt dafür die Auswahl von je schützenswertem Bauteil passenden Sicherheitsmerkmalen auf Basis technischer sowie wirtschaftlicher Kriterien. Dafür werden neue, für diesen Prozess passende Methoden entwickelt. Die drei folgenden Abschnitte sind mit ihren Inhalten nebenläufig zu sehen: Kombination von Originalitäts- und Identitätskennzeichen zur Erzeugung eines Unikatkennzeichens, RFID als Sicherheitsmerkmal und Hinweise zum Auf- / Einbringen eines Sicherheitsmerkmals auf / in die schützenswerten Bauteile. Alle Inhalte dieses Kapitels werden mit durchgängigen Beispielen begleitet. Abschließend erfolgt die Zusammenfassung der Ergebnisse und der Abgleich mit den Anforderungen aus Kapitel fünf.

In Kapitel acht wird für die mit Sicherheitsmerkmalen gekennzeichneten schützenswerten Bauteile das gesamte technische System zum Produktpiraterieschutz des Logistiknetzwerks sowie der Maschinen des Originalherstellers konzipiert. Nach Bildung der Einheit aus Bauteil, Identitäts- und Sicherheitsmerkmal erfolgt deren Authentifizierung am IP-Punkt. Der Aufbau und die Funktionsweise dieser IP-Punkte wird schematisch dargestellt, der Informationsfluss und die Datenentstehung aufgezeigt sowie eine formale Definition für die IP-Punkte erarbeitet. Die Einbindung der IP-Punkte im gesamten verteilten IT-System zur Datenarchivierung und -auswertung erfolgt anschließend. Das gesamte entwickelte Produktpiraterie-Schutzsystem kann als Neuentwicklung aufgebaut, jedoch auch als Erweiterung des EPCglobal Networks implementiert werden. Zudem ist das System für Unikatkennzeichen konzipiert, es können aber auch Originalitätskennzeichen Verwendung finden. Wie dies möglich ist, wird theoretisch aufgezeigt und mittels Beispielen verdeutlicht. Abschließend erfolgt in Kapitel acht die Zusammenfassung der Ergebnisse sowie der Abgleich mit den Anforderungen aus Kapitel fünf.

Nach der Entwicklung des gesamten technischen Produktpiraterie-Schutzsystems wird in Kapitel neun dargestellt, wie innerhalb des Gesamtsystems lokal wie auch zentral passende Systemreaktionen erzeugt und weitere Funktionen in Form von Zusatznutzen implementiert werden können. Dies wird an Beispielen verdeutlicht. Zudem werden die Ergebnisse einer rechtlichen Bewertung des gesamten technischen Produktpiraterie-Schutzsystems vorgestellt und die rechtliche Voraussetzungen für dessen Einsatz aufgezeigt. Auch dieses Kapitel schließt mit einer Zusammenfassung und dem Abgleich der erarbeiteten Inhalte mit den Anforderungen aus Kapitel fünf.

Die Arbeit wird in Kapitel zehn zusammengefasst. Es folgt ein Ausblick und der Epilog.

Abbildung 1-9: Inhaltlicher Aufbau der Arbeit, Kapitel eins bis sechs

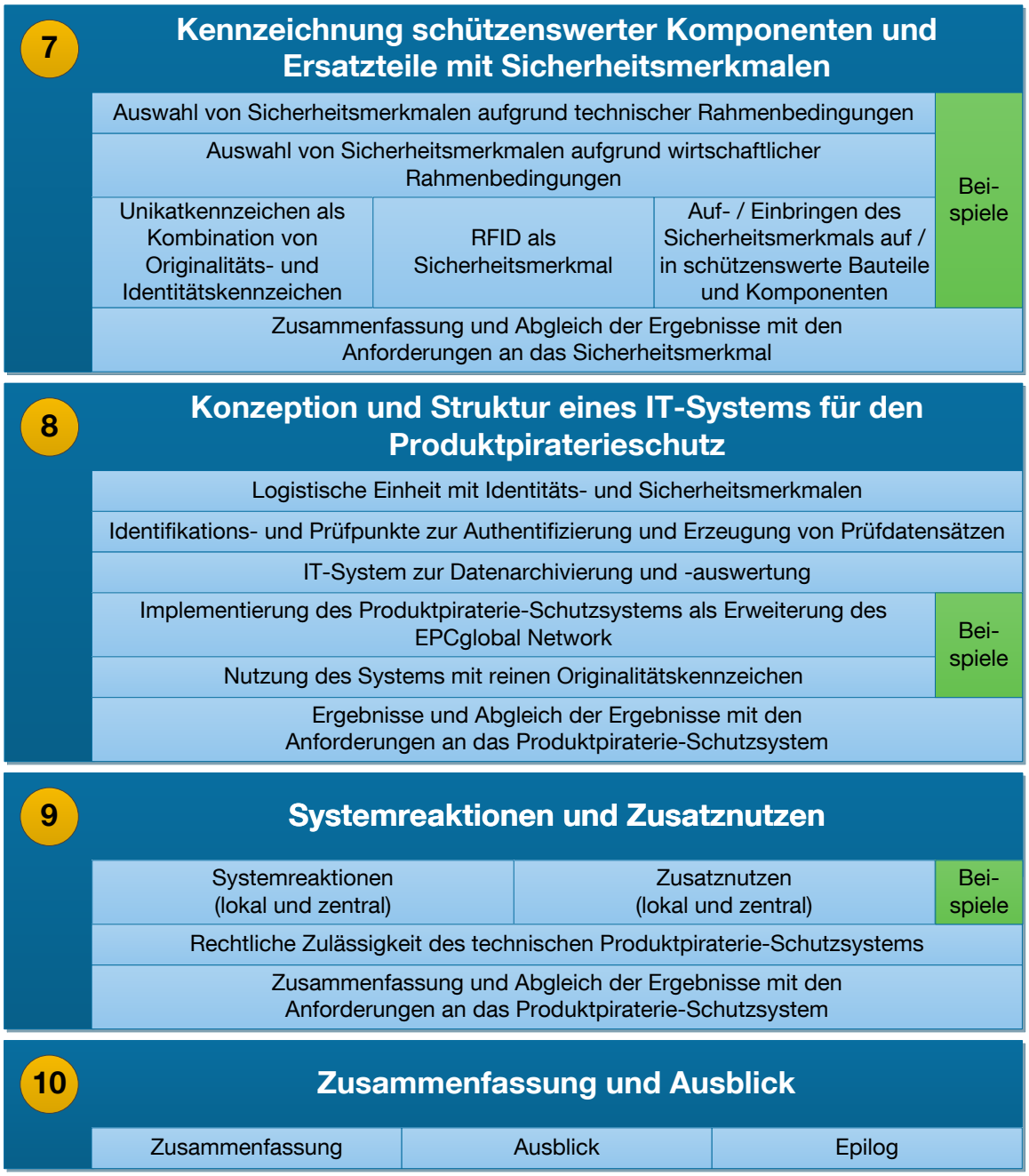


Abbildung 1-10: Inhaltlicher Aufbau der Arbeit, Kapitel sieben bis zehn

2 Begriffsbestimmung und Abgrenzung des Untersuchungsbereichs

Für die begriffliche Kohärenz in der vorliegenden Arbeit werden in diesem Abschnitt grundlegende Begriffe im Themenbereich Produkt- und Markenpiraterie definiert. Zudem werden nach der Darstellung der Motivation von Produktpiraten und den möglichen Folgen aus Produkt- und Markenpiraterie eine allgemeine Übersicht über Handlungsalternativen für Unternehmen sowie ein Überblick über die juristischen Maßnahmen gegeben.

2.1 Die Begriffe Produktpiraterie und Markenpiraterie

In kaum einem anderen Bereich des Geistigen Eigentums herrscht ein solches Begriffswirrwarr wie bei der Benennung gewerblich begangener Schutzrechtsverletzungen. Daher wird in dieser Arbeit zunächst eine begriffliche Grundlage geschaffen, in der die einzelnen Begriffe definiert und aufgrund des rechtlich gegebenen Rahmens sowie ihrer semantischen Belegung eingeordnet werden. Dies stellt eine kohärente Begriffsbelegung und -verwendung innerhalb dieser Arbeit sicher, soll aber gleichzeitig der weiteren Wissenschaft und Forschung im Themenbereich Produkt- und Markenpiraterie dienen. In diesem Abschnitt werden zunächst die beiden grundlegenden Begriffe „Produktpiraterie“ und „Markenpiraterie“ definiert. Die Definition weiterer Begriffe der Begriffswelt erfolgt in Abschnitt 2.7.

Ann und Hauck stellen in [Gün-11b] den rechtlichen Hintergrund für den Begriff Produktpiraterie eindeutig dar. Dabei werden europäische wie auch deutsche Gesetze als Grundlage verwendet: Produktpiraterie liegt vor in Fällen „der vorsätzlichen und gewerbsmäßigen und somit massenhaften Verletzung fremder Schutzrechte […]. Ob eine Patentverletzung tatsächlich vorliegt, richtet sich nach den Voraussetzungen des § 139 PatG.“ [Gün-11b S. 14].

Diese sehr enge Definition von Produktpiraterie stimmt zwar mit der Gesetzgebung überein, deckt sich aber nicht mit dem gebräuchlichen Begriffsverständnis. Der im herkömmlichen Sprachgebrauch verwendeten Schutzrechtsverletzung fehlen der im Gesetz benannte hohe Unrechtsgehalt als auch die Zielgerichtetheit, d. h. die Schutzrechtsverletzung ist nicht „das Geschäftsmodell des Verletzers, sie ist nicht

Hauptinhalt seiner Tätigkeit.“ [Gün-11b S. 14 f.]. Daher wird diese gesetzeskonforme Definition von Produktpiraterie analog zu *Wildemann* etwas weiter gefasst und gleichzeitig aufgeteilt in:

Produktpiraterie:
Bei Produktpiraterie wird Ware nachgeahmt, „für welche der Originalhersteller Verfahrens-, Erfindungs- oder Designrechte besitzt, er also Patentinhaber oder Urheber ist, oder ein gebrauchs- beziehungsweise geschmacksmusterrechtlicher Schutz besteht.“ [Wil-07 S. 131]

Markenpiraterie:
„Unter Markenpiraterie versteht man das illegale Verwenden von Zeichen, Logos, Namen und geschäftlichen Bezeichnungen, die der Hersteller zur Kennzeichnung seiner Ware verwendet. Verletzt wird hier das Markenrecht des Inhabers der Marke.“ [Wil-07 S. 131]

2.2 Motivation der Produktpiraten

Auf den chinesischen Philosophen Konfuzius[4] geht das folgende Zitat zurück: „Der Mensch hat dreierlei Wege klug zu handeln: erstens durch Nachdenken, das ist der edelste, zweitens durch Nachahmen, das ist der leichteste, und drittens durch Erfahrung, das ist der bitterste.“ [Bro-12c, Zit-12]

Die Wahl des zweiten Weges liegt für Produktpiraten und Fälscher nicht nur, weil es der leichteste ist, am nächsten, sondern auch aus zwei weiteren einfachen Gründen. Einerseits sind die Gewinnspannen in der Produkt- und Markenpiraterie sehr hoch. Produktpiraten des produzierenden Gewerbes erzielen aufgrund enormer Kostenpotenziale gegenüber den Aufwendungen des Originalherstellers (siehe hierzu [Wil-07 S. 11 ff.]) „oftmals eine bis zu 10fache Marge“ [Wil-07 S. 13]. Durch Produktpiraterie lassen sich somit exorbitante Gewinne erzielen [Blu-06 S. 77], die in manchen Segmenten sogar höher als im Drogenhandel sind [Fuc-06 S. 18]. Andererseits ist das Vergeltungsrisiko, das sich berechnet als das mathematische Produkt aus der Ent-

[4] * Qufu 551, † ebenda 479 v. Chr.

deckungswahrscheinlichkeit und der Höhe der Strafen, dem sogenannten Sanktionsausmaß, sehr gering [Blu-06 S. 77, Nee-07 S. 53] und sogar sinkend [Hub-10].

Kombiniert mit der empirischen Erkenntnis, dass Produktpiraten vorwiegend innovative oder bekannte Unternehmen bedrohen, dass Marken und Produkte nur dann kopiert werden, wenn mit hohen Absatzzahlen und / oder einer hohen Marge gerechnet werden kann [Wil-07 S. 10], liegt es nahe, dass der deutsche Maschinenbau „immer häufiger […] von Produktpiraterie betroffen“ ist [Fra-12, VDMA-12b].

2.3 Schäden und Folgen von Produkt- und Markenpiraterie

Produkt- und Markenpiraterie schädigt den Originalhersteller teils direkt, teils indirekt. Für Kunden können negative Folgen und sehr ernste Schädigungen entstehen. Auch das Gemeinwesen leidet.

In den folgenden drei Abschnitten wird ein Überblick über mögliche Schäden und Folgen gegeben. Dabei ist feststellbar, dass all diese Schäden und Folgen aufgrund von Produkt- und Markenpiraterie im Allgemeinen, aber identisch auch im Bereich des Maschinen- und Anlagenbaus auftreten.

Die umfangreiche Liste in den Abschnitten 2.3.1, 2.3.2 und 2.3.3 stellt eine Konsolidierung von Angaben aus den folgenden Quellen dar: [Abe-11 S. 13 ff., Blu-06 S. 62 ff., Fuc-06 S. 47 ff., Gau-10 S. 4, Gau-12 S. 20 ff., Kro-06 S. 17 ff., OECD-08 S. 102, Par-12, Ste-11a S. 69 ff., Wel-07 S. 48 ff., Wil-07 S. 5 ff.].

2.3.1 Schadensarten für Hersteller

Die Schadensarten für die Hersteller lassen sich einteilen in unmittelbare und mittelbare Schadensarten.

Unmittelbare Schadensarten:

- Umsatz- und Gewinnverluste
- Verminderte Einnahmen der Rechteinhaber aus Lizenzgebühren
- Kosten für Anmeldung, Verfolgung und Durchsetzung von Schutzrechten
- Kosten für Schutzmaßnahmen

Mittelbare Schadensarten:

- Druck auf das Preisniveau und Preisverfall
- Imageverlust, Erosion der Marken und des Unternehmenswerts
- Kosten für ungerechtfertigte Kundendiensteinsätze, Gewährleistungsansprüche, Garantieforderungen
- Kosten für die begründete Ablehnung von Forderungen aufgrund Verfügbarkeitsgarantien, Regressforderungen und Produkthaftungsansprüchen
- Verlust eigenen Know-hows
- Verlust des Know-how- und Innovationsvorsprungs
- Verlust von Marktanteilen
- Verlust von Absatzmärkten
- Verlust von Zukunftsmärkten
- Negative Auswirkungen auf Forschung und Entwicklung sowie andere kreative Aktivitäten
- Verringerung der Unternehmensinvestitionen
- Verlangsamung des eigenen technischen Fortschritts
- Schwächung der eigenen Wettbewerbsfähigkeit
- Einschränkung der Geschäftstätigkeit der Rechteinhaber, erhöhtes Konkursrisiko
- Insolvenz
- Haftung wegen unterlassener Pirateriebekämpfung

2.3.2 Folgen für Verbraucher

- Wirtschaftliche Schäden durch einen, in der Regel verminderten Verbrauchernutzen
- Gefahr für Sicherheit, Gesundheit und Leben durch Einsatz von Kopien, z. B. durch kopierte Arzneimittel, Flugzeug-, Automobil-, Maschinenersatzteile, Spirituosen, Spielzeuge, Babynahrung
- Blamage eines getäuschten Verbrauchers in seinem Umfeld
- Strafrechtliche Verfolgung als Käufer von Pirateriewaren
- Strafrechtliche Verfolgung als Inverkehrbringer von Pirateriewaren bei Weiterverkauf

2.3.3 Auswirkungen auf das Gemeinwesen

Die Auswirkungen auf das Gemeinwesen lassen sich aufteilen in Auswirkungen auf staatlicher Ebene sowie sozioökonomische Auswirkungen.

Auswirkungen auf staatlicher Ebene:

- Steuerausfälle
- Fehlende Sozialversicherungseinnahmen
- Kosten für Initiativen zur Sensibilisierung der Öffentlichkeit
- Kosten für personelle und sachliche Mittel für Gerichte, Zoll- und Strafverfolgungsbehörden
- Korruption: Schwächung der Effektivität öffentlicher Institutionen, die mit der Rechtsdurchsetzung und der damit verbundenen staatlichen Aktivitäten betraut sind durch Bestechung und Erpressung von öffentlichen Amtsträgern mit dem Ziel der Erleichterung oder Unterstützung des Piraterie-Geschäfts

Allgemeine sozioökonomische Auswirkungen:

- Schädigung der Reputation der Ursprungs- und Zielländer von Pirateriewaren
- Schlechtes Investitionsklima in den Ursprungsländern von Pirateriewaren und somit Verlust von Arbeitsplätzen
- Handelssanktionen gegen Herkunftsländer
- Schlechtere Arbeitsbedingungen und Missachtung des Arbeitsschutzes in rechtsverletzenden Unternehmen
- Fehlender Umweltschutz und Schäden für die Umwelt durch Nicht-Einhaltung entsprechender Vorschriften in den rechtsverletzenden Unternehmen
- Stärkung krimineller Netzwerke aufgrund des verstärkten Kapitalzuflusses aus Geschäften der Produkt- und Markenpiraterie in den Herkunftsländern
- Verlust von Arbeitsplätzen in den Ländern der Originalhersteller und somit steigende Sozialversicherungsausgaben

2.4 Handlungsmöglichkeiten für Unternehmen

Die Handlungsalternativen für betroffene Unternehmen, aktiv oder reaktiv gegen Produkt- und Markenpiraterie vorzugehen, sind sehr vielfältig.[5] Nach *Wildemann* sowie *Fuchs* lassen sich dabei bestimmte Kategorien benennen, in welche die existierenden Maßnahmen eingeordnet werden können. Im Folgenden werden diese Kategorien und jeweils passende Beispiele genannt [Wil-07 S. 32 - 168, Fuc-06 S. 160 ff., S. 291]:

- Nichts / Duldung:
    - keine Maßnahmen aufgrund der fallspezifischen Kosten-Nutzen-Bewertung, jedoch ständige Beobachtung
- Produktbezogene Ansätze:
    - Produkt-, Produktionsprogrammgestaltung
    - Entwicklung und Entwicklungsprozesse, kurze Innovationszyklen
- Produktions- / technologiebezogene Ansätze:
    - Entwicklungs-, Produktions-, Vertriebsprozesse
    - Produktkennzeichnung und Authentifizierung
- IT-Sicherheit:
    - Sicherheit von Produktsoftware oder gespeicherten (Produkt-)Daten
    - Schutz der Kommunikation
- Betriebswirtschaftliche Ansätze:
    - Bewusster Verzicht auf Markteintritt
    - Eigenes günstiges Alternativangebot zum teuren Stammprodukt
    - Pakete aus Produkten und Dienstleistungen
- Juristische Ansätze:
    - Schutzrechtsanmeldung und -durchsetzung
    - Vertraglicher Know-how-Schutz
- Politik:
    - Einflussnahme auf Verbraucherverhalten und Politik
- Integrierte Gesamtstrategien:
    - Kombination und paralleler Einsatz einzelner Strategien

[5] umfangreiche Maßnahmensammlungen und -beschreibungen finden sich beispielsweise in den Quellen [Gau-12, Hei-12, Lin-12, Mei-11, Wil-07]

Wie in Abschnitt 1.2, S. 6 dargestellt, wird in der vorliegenden Arbeit die Maßnahme „Produktkennzeichnung und Authentifizierung“ als Teil der „Produktions- / technologiebezogenen Ansätze“ näher untersucht, ein technisches Produktpiraterie-Schutzsystems entwickelt und die Möglichkeiten der Ausgestaltung detailliert beschrieben. Neben dieser Maßnahme gibt es jedoch mehr als 200 weitere Schutzmaßnahmen [Kok-02, Abe-10 S. 18, Gau-10 S. 28]. Zur Auswahl der für ein Unternehmen und dessen spezifische Situation passenden Schutzmaßnahmen gibt es verschiedene Ansätze und Verfahren (siehe z. B. [Abe-10 S. 25 ff., KIT-12a, Mei-11, Sch-10a]). Der Ansatz, Produktpiraterie mit juristischen Mitteln zu bekämpfen, ist jedoch am weitesten verbreitet [Abe-11 S. 20, Fuc-06 S. 117, Lin-12 S. 102, Wil-07 S. 8]. Aus diesem Grund und da die juristischen Zusammenhänge auch Grundlage für die vorliegende Arbeit bilden, werden diese im Folgenden näher betrachtet.

2.5 Juristische Maßnahmen und deren Grenzen

„So lange ein Leistungsergebnis nicht durch ein Immaterialgüterrecht geschützt ist, gilt im Grundsatz, dass die Nachahmung nicht untersagt werden kann“ [Wel-07 S. 61]. Dies gilt auch im internationalen Umfeld. Grundvoraussetzung für den Einsatz juristischer Maßnahmen ist also der Erwerb eines Schutzrechts, das mit den entsprechenden juristischen Mitteln verteidigt werden darf (siehe Abbildung 2-1).

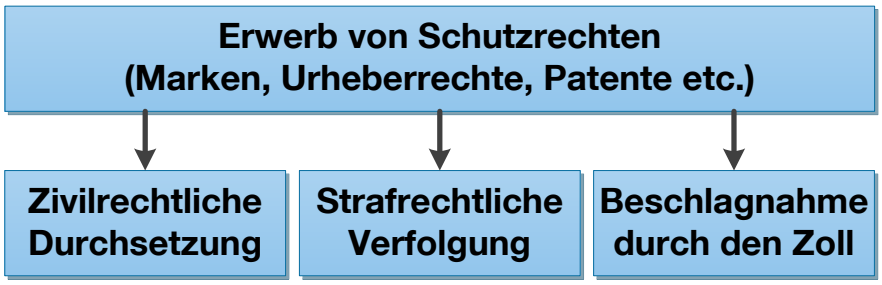


Abbildung 2-1: System rechtlicher Maßnahmen bei Verteidigung von Schutzrechten [Wel-07 S. 59]

Dabei ist die landesspezifische Gesetzgebung zu beachten. Grundsätzlich gibt es aber internationale Übereinkommen, die in den Staaten, die beigetreten sind, einen bestimmten Schutz für geistiges Eigentum sicherstellen [Wel-07 S. 61].[6] Bei der Anmeldung von Schutzrechten muss beachtet werden, dass diese sowohl in Produktions- und Vertriebsländern, insbesondere aber auch in Ländern, in denen Fäl-

[6] In der Einführung, S. 16 ist dafür ein kleiner Überblick gegeben.

schungen hergestellt und verkauft werden, angemeldet werden sollten [Wel-07 S. 61]. In Deutschland kommen im Zusammenhang mit Produkt- und Markenpiraterie die in Tabelle 2-1 angeführten Gesetze zur Anwendung.

Klar ist, dass juristische Mittel und Maßnahmen das Rückgrat im Kampf gegen Produktpiraterie bilden [Fuc-06 S. 183 ff., Wil-07 S. 8, Wel-07 S. 61, Hof-10 S. 86]. Jedoch, auch wenn die „Anmeldung von gewerblichen Schutzrechten […] für die erfolgreiche Bekämpfung von Produktpiraterie essentiell“ ist [Wel-07 S. 6], greift diese Maßnahme alleine zu kurz [BMBF-12, Lin-12 S. 102, Hof-10 S. 86, Wil-07 S. 8]. Denn „juristische Maßnahmen sind reaktiv, sie laufen der Entwicklung immer nur hinterher“ [Fuc-06 S. 117]. Schutzrechte werden nämlich erst wirksam, wenn ihre Beachtung bzw. Nicht-Übertretung ständig überwacht und eingefordert, schlimmstenfalls eingeklagt wird und daher entfalten sie „ihre Wirkung meist erst, nachdem der Schaden bereits eingetreten ist“ [Wil-07 S. 8].

Zudem ist der Know-how-Schutz bei alleiniger Anwendung juristischer Mittel „hoffnungslos fragmentiert“ [Abe-11 S. 21]. Dies ist schon alleine deshalb klar, weil es viele Komponenten und Ersatzteile im Maschinen- und Anlagenbau gibt, die nicht durch ein Patent geschützt werden können: Der Stand der Technik ist nicht patentierbar [DPMA-12]. Gerade bei den international arbeitenden Unternehmen des Maschinen- und Anlagenbaus braucht es daher neben den juristischen noch weitere Maßnahmen, um dem Problem der Produkt- und Markenpiraterie Herr zu werden [Abe-11 S. 20].

Tabelle 2-1: Schutzrechte [Bun-87, Bun-97, DPMA-08 S. 3, Sit-06 S. 31 f., Wel-07 S. 61]

	Gesetzliche Grundlage		Schutz-gegenstand	Schutzvoraus-setzungen	Schutzbeginn	Schutz-dauer
	Abkürzung, Kurztitel	Langtitel				
Gewerblicher Rechtsschutz	GebrMG: Gebrauchs-mustergesetz	-	technische Erfindung	Neuheit, erfinderischer Schritt, gewerbliche Anwendbarkeit	mit der Eintra-gung in das jeweilige Register	3 + 3 + 2 + 2 Jahre
	GeschmMG: Geschmacks-mustergesetz	Gesetz über den recht-lichen Schutz von Mustern und Modellen	Design repräsen-tiert als gewerb-liches Muster (Flächenform) oder Modell (Raumform)	Neuheit, Eigen-art, gewerb-liche Anwend-barkeit	mit der Eintra-gung in das jeweilige Register	5 + 5 + 5 + 5 Jahre
	HalblSchG: Halbleiter-schutzgesetz	Gesetz über den Schutz der Topogra-phien von mikroelek-tronischen Halbleiter-erzeugnissen	dreidimensiona-le Topographie eines Halbleiter-erzeugnisses	Eigenart	am Tag der Anmeldung oder der ers-ten geschäft-lichen Ver-wendung (§5 HalblSchG)	10 Jahre ab Veröf-fentlichung
	MarkenG: Marken-gesetz	Gesetz über den Schutz von Marken und sonstigen Kennzeichen	Kennzeichen bzw. Marke für eine Ware, Dienstleistung oder Ausstattung	Unterschei-dungskraft, fehlendes Freihaltebe-dürfnis	mit der Eintragung in das jeweilige Register	alle 10 Jahre um weitere 10 Jahre unbe-grenzt ver-längerbar
	PatG: Patentgesetz	-	technische Erfindung	Neuheit, erfinderische Tätigkeit	mit der Veröf-fentlichung im Patentblatt	20 Jahre gültig
	SortSchG: Sortenschutz-gesetz	-	Pflanzen-züchtungen	Neuheit, Unterscheid-barkeit, Homogenität, Beständigkeit	Ab Bekannt-machung des Antrags (§ 37 SortSchG)	25 bis 30 Jahre nach Er-teilung
Kunst-schutz	UrhG: Urheber-rechtsgesetz	Gesetz über Urheberrecht und verwand-te Schutz-rechte	Werke der Mu-sik, Kunst, Litera-tur, Fotographie, Filmwerke, Soft-ware, Daten-banken etc.	persönliche geistige Schöpfung	entsteht formlos automatisch mit der Schöpfung des Werkes	Gültig bis 70 Jahre nach dem Tod des Urhebers
Wett-bewerb	UWG: Gesetz gegen den unlaute-ren Wettbe-werb	-	Greift, wenn kein Schutz durch eines der anderen Spezialgesetze besteht. Die Generalklausel des UWG, der § 1, verbietet Wettbewerbshandlungen, die gegen die "guten Sitten" verstoßen.			

2.6 Untersuchungs- und Einsatzbereich

Um dem Problem „Produkt- und Markenpiraterie im Komponenten- und Ersatzteilgeschäft“ zu begegnen, wird in dieser Arbeit ein technisches Schutzsystem erarbeitet, das ergänzend zu juristischen Maßnahmen zum Einsatz kommen soll. Basis bilden kopiersichere und / oder markenrechtlich geschützte Kennzeichen, die auf Originale aufgebracht oder integriert eine dauerhafte Unterscheidbarkeit zwischen Original und Kopie ermöglichen. Gleichzeitig sollen diese Sicherheitsmerkmale ein Tracking&Tracing ermöglichen, um die Originale in der Supply-Chain verfolgen und rückverfolgen zu können (siehe Abschnitt 1.2.2, S. 8).

Die folgende Aufzählung zeigt auf, was im Maschinen- und Anlagenbau gefälscht wird [Fuc-06 S. 6, Kle-10 S. 131 ff., VDMA-12a S. 11]:

- Komponenten / Teile
- Ersatzteile
- Verpackungen
- Anleitungen
- Software
- Marken
- Designs
- Dienstleistungen
- Geschäftskonzepte
- Produkte
- Ganze Maschinen

Da das zu entwickelnde technische System mit Kennzeichnung und Authentifizierung von Originalwaren arbeiten soll (siehe Abschnitt 1.2.2, S. 8), sollen gegenständliche Objekte markiert und anschließend authentifiziert werden. Ein solches System ist daher für den Schutz aller hergestellten Komponenten und Ersatzteile, prinzipiell aber auch für Verpackungen oder Anleitungen geeignet.

Was mit diesem System nicht zu schützen ist, sind immaterielle Güter wie Software, Marken, Designs, Dienstleistungen und Geschäftskonzepte. Hier müssen andere Maßnahmen zum Einsatz kommen (siehe Abschnitte 2.4 und 2.5). Und obwohl es sich bei alleinstehenden Produkten oder Maschinen auch um „Gegenstände“ handelt, könnte dieses System nicht erkennen oder gar verhindern, dass diese in irgendeinem Land der Welt nachgebaut werden.

Der Fokus in dieser Arbeit liegt daher auf den für den Maschinen- und Anlagenbau wirtschaftlich so wichtigen Komponenten und Ersatzteilen (siehe Abschnitt 1.1.2, S. 2 mit Abbildung 1-1, S. 3). Es wird jedoch davon ausgegangen, dass dieses System auch in anderen Fällen wirksam eingesetzt werden kann.

2.7 Begrifflichkeiten im Themenbereich der Produkt- und Markenpiraterie

In Abschnitt 2.1 wurde bereits festgestellt, dass es im Themenbereich der Produkt- und Markenpiraterie ein großes Durcheinander an Begriffen, deren Definitionen und Bedeutungen und damit deren Verwendung gibt. Um eine einheitliche Basis für die vorliegende Arbeit aber auch darüber hinaus für weitere Arbeiten im Themenbereich zu schaffen, wird die in Abschnitt 2.1 mit den Begriffen „Produktpiraterie“ und „Markenpiraterie“ begonnene Begriffsdefinition und -ordnung in diesem Abschnitt fortgesetzt.

2.7.1 Grundlegende Begriffe

Grundlegend für das Thema Produkt- und Markenpiraterie sind die Begriffe „Identität“ und „Identifizierung“. Diese sowie weitere hier definierte Begriffe wurden durch den Autor teils schon in *Günthner et al.* vorveröffentlicht [Gün-08]. Bei Verwendung dieser Vorveröffentlichungen ist die Quelle [Gün-08] jeweils angegeben[7]:

Identität:
„Identität ist die Summe aller Merkmale, anhand derer sich ein Objekt von anderen unterscheiden lässt, und erlaubt eine eindeutige Identifizierung.“ [Gün-08 S. 24]

Identifizierung:
„Identifizierung ist der Vorgang des eindeutigen Erkennens eines Objektes anhand dessen, …

- … was es ist: sogenannte **existenzielle Identifizierung** anhand eindeutiger objekteigener Merkmale.
- … was es hat: sogenannte **possessive Identifizierung** anhand eindeutiger Merkmale, die es besitzt.
- … was es weiß: sogenannte **kognitive Identifizierung** anhand eindeutigen Wissens, das es hat.“ [Gün-08 S. 24]

[7] Die Definition für „Identifizierung“ wurde inhaltliche identisch zeitgleich von Rankl und Effing entwickelt [siehe Ran-08 S. 179].

Übertragen auf den Menschen erfolgt die existenzielle Identifizierung anhand biometrischer Merkmale beispielsweise mittels Lichtbild, Augenfarbe oder Unterschrift [Beh-01 S. 13, BMI-13, BSI-13a, § 5 PAuswG in Bun-09]. An Ländergrenzen erfolgt Identifizierung der Reisenden possessiv anhand des mitgeführten Reisepasses. In IT-Systemen und -Anwendungen erfolgt in der Regel eine kognitive Identifizierung durch ein Passwort, das nur der Nutzer selbst kennt.

In den Themenbereich Produkt- und Markenpiraterie gehören auch die Begriffe „Kennzeichen“ und „Kennzeichnung“:

Kennzeichen:
Kennzeichen sind alle Zeichen, insbesondere Wörter (einschließlich Namen), Abbildungen, Buchstaben, Zahlen, Gesten, Hörzeichen, Düfte, Geschmacksmuster, dreidimensionale Gestaltungen einschließlich der Form oder sonstige Aufmachungen einschließlich Farben und Farbzusammenstellungen, die geeignet sind, Personen, Gegenstände oder Handlungen von anderen zu unterscheiden. [in Anlehnung an § 3 Abs. 1 MarkenG, BMJ-13e]

Kennzeichnung:
Die „Kennzeichnung ist das Ausstatten eines Objektes mit einem Kennzeichen, um eine Identifizierung zu ermöglichen.“ [Gün-08 S. 25]

Kennzeichen wiederum können eingeteilt werden in „Identitätskennzeichen“, „Originalitätskennzeichen“ und „Unikatkennzeichen“; der Begriff „Sicherheitsmerkmale“ umfasst Originalitäts- und Unikatkennzeichen:

Identitätskennzeichen:
Kennzeichen zur Serialisierung von Gegenständen ohne fälschungssichere Merkmale.

Originalitätskennzeichen:
„Kennzeichen mit fälschungssicheren Merkmalen.“ [Gün-08 S. 25]

Unikatkennzeichen:
„Kennzeichen mit fälschungssicheren, einmaligen Merkmalen.“ [Gün-08 S. 25]

Sicherheitsmerkmal:
Sammelbegriff für Elemente auf oder in Dokumenten oder Objekten mit dem Ziel der Echtheitserkennung und des Kopierschutzes [in Anlehnung an Gie-13a]. Sicherheitsmerkmale können Originalitäts- oder ein Unikatkennzeichen sein.

Insbesondere ist es möglich, serialisierte Identitätskennzeichen mit Originalitätskennzeichen zu kombinieren, um ein Unikatkennzeichen zu erzeugen (siehe Abschnitt 7.3, S. 158).

Schließlich fehlen noch die Begriffe „Authentisierung“ und „Authentifizierung“ als Ergänzung zur Identifizierung:

Authentisierung:
Der Vorgang des Nachweises der behaupteten Identität einer Instanz durch existenzielle, possessive oder kognitive Merkmale wird als Authentisierung bezeichnet. [Ran-08 S. 178]

Authentifizierung:
Der aktive Vorgang des Nachweises der eigenen Identität gegenüber einer anderen Instanz durch existenzielle, possessive oder kognitive Merkmale wird als Authentifizierung bezeichnet. [Ran-08 S. 178]

Einseitige Authentisierung (unilateral):
Bei der einseitigen Authentisierung ist im Gutfall die Authentizität eines der beiden Kommunikationspartner sichergestellt. [Ran-08 S. 179]

Gegenseitige Authentisierung (mutual):
„Bei der gegenseitigen Authentisierung sind […] im Gutfall beide Partner authentisch." [Ran-08 S. 179]

Die Authentifizierung oder Authentisierung führen zu einem Ergebnis: Ein vorliegendes und geprüftes Objekt ist ein Original oder es ist kein Original. Dies sind die zentralen Begriffe für die vorliegende Arbeit, da es um die Feststellung der Originalität von Waren geht. Der Unterschied zwischen Authentifizierung und Authentisierung besteht darin, ob der Nachweis der eigenen Identität aktiv durch die Instanz selbst oder passiv durch eine prüfende Instanz erfolgt. Im allgemeinen Sprachgebrauch wird dieser Unterschied jedoch kaum gemacht, weshalb in der vorliegenden Arbeit auch vereinfachend der Begriff Authentifizierung verwendet wird.

Zur Ergänzung der Begrifflichkeiten werden auch „Authentizität" und „Autorisierung" definiert:

Authentizität:
„Authentizität bezeichnet […] die Echtheit und Unverändertheit einer Instanz oder Nachricht“ [Ran-08 S. 179]

Autorisierung:
„Die Prüfung, ob eine bestimmte Aktion ausgeführt werden darf, wird „Autorisierung“ genannt, d. h. jemand wird zu etwas ermächtigt.“ [Ran-08 S. 179]

2.7.2 Piraterieware, Fälschungen und Plagiate

Zur Bezeichnung von nicht-originalen Waren aus Produkt- und Markenpiraterie gibt es aufgrund der vielfältigen Formen und Ausprägungen sehr viele verschiedene Begriffe. Diese sind in der Literatur oftmals nicht einheitlich belegt. Daher wird hier ein Vorschlag erarbeitet, der die Begriffswelt auf eine neue Art ordnet. Es wird ein Schema vorgeschlagen, das einfach und logisch aufgebaut und somit leicht verständlich ist. Hierfür wurden entsprechend gewichtige Quellen [Blu-06, Bro-12a, Bro-12d, Bro-12e, Bro-12f, Bro-12g, Bro-12h, Mei-11, Nee-07, Spr-12, Wel-07, Wil-07] analysiert, ausgewertet und die Begriffe in das Schema in Abbildung 2-2 eingeordnet. Dieses Schema soll auch dazu dienen, weitere Begriffe sinnvoll in den Gesamtzusammenhang einordnen zu können.

Das neue Schema teilt Waren in zwei konträre Gruppen ein: Originalwaren und Kopien. Dabei handelt es sich bei Originalwaren um alle Produkte, die der Originalhersteller selbst herstellt oder in Lizenz herstellen lässt. Dieser Gruppe stehen gegenüber alle Produkte, die ohne Kenntnis oder Einwilligung des Originalherstellers produziert werden. Sämtliche in Abbildung 2-2 eingeführten Begriffe werden im Anschluss an die Abbildung definiert.

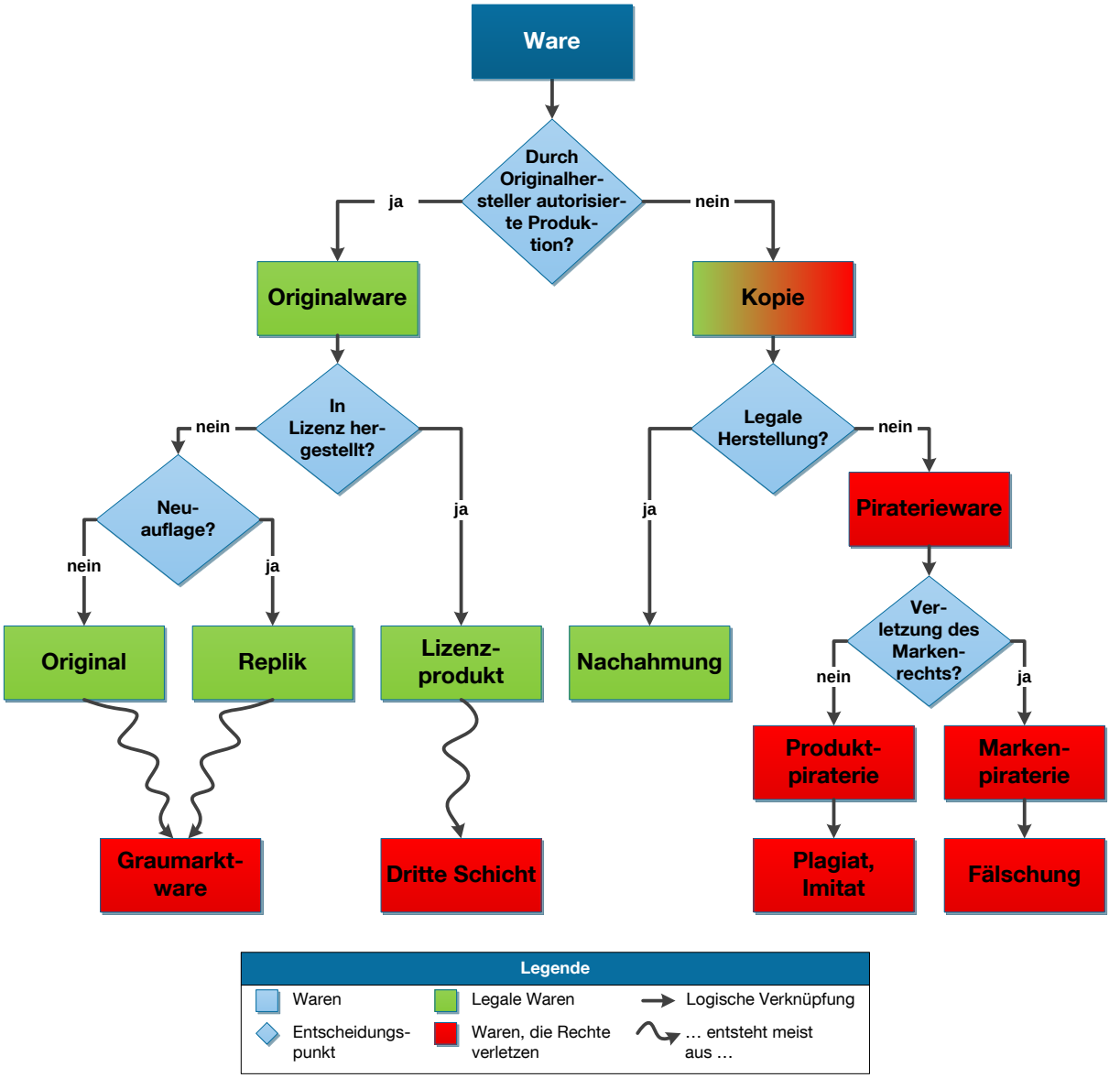


Abbildung 2-2: Schema zur Einordnung von Begriffen im Themenbereich der Produkt- und Markenpiraterie [8]

[8] Produkt- und Markenpiraterie kann auch in einer Kopie gleichzeitig auftauchen [Wel-07 S. 59]

Ware:
Eine Ware ist eine „bewegliche Sache, die Gegenstand des Handelsverkehrs ist oder die nach der Anschauung des Verkehrs als Gegenstand des Warenumsatzes in Betracht kommen könnte“. Beinhaltet ist dabei auch beispielsweise Elektrizität, nicht aber Grundstücke. [Spr-12]

Originalware:
Alle Waren, die in einer, durch den Urheber, also den Originalhersteller autorisierten Produktion hergestellt wurden. Diese können eingeteilt werden in Originale, Replik und Lizenzprodukt.

Original:
Ein Objekt, welches „das ursprüngliche, echte Exemplar“ ist, die vom Urheber stammende Fassung. [Bro-12f]

Replik:
Die vom Urheber selbst hergestellte Wiederholung des Originals. [in Anlehnung an Bro-12h]

Lizenzprodukt:
Ein Lizenzprodukt ist ein Produkt, das in Lizenz hergestellt wurde. Dieser Produktion liegt ein Lizenzvertrag zugrunde und erteilt die Erlaubnis, ein Patent, eine Marke oder andere gewerbliche Schutzrechte (siehe Tabelle 2-1) zu nutzen. [Bro-12d]

Kopie:
Alle Waren aus einer, nicht vom Originalhersteller autorisierten Produktion werden zusammenfassend als Kopie bezeichnet. Dieser Sammelbegriff ist insbesondere deshalb sinnvoll, weil jegliche Form von Kopien seitens des Originalherstellers unerwünscht sind und er sich mit seinen Originalwaren klar davon abgrenzt.

Nachahmung (auch Nachahmerprodukt):
Die möglichst genaue Kopie eines Gegenstandes. Die Kopie ist erlaubt, solange sie nicht ein „durch Sondergesetz geschütztes Rechtsgut verletzt, z. B. Urheberrecht, Geschmacksmuster, Gebrauchsmuster, Patent oder Kennzeichen“ (siehe Tabelle 2-1). [Bro-12e]

Piraterieware:
Der Begriff Piraterieware umfasst alle Waren, welche Rechte des Originalherstellers verletzen (siehe Tabelle 2-1). [in Anlehnung an Wil-07 S. 1]

Plagiat:
Plagiate sind Waren, denen die eigene Urheberschaft unterstellt wird [in Anlehnung an Bro-12g] und sehr genau nach dem Vorbild einer Originalware hergestellt wurden. Insbesondere tragen diese Waren nicht den Markennamen des Originalherstellers. [Blu-06 S. 34, Mei-11 S. 23]

Imitat:
Ein Imitat ist ein Produkt, das zeitlich nach der Originalware auftritt, aus Sicht des Kunden eine ähnliche Anwendungsfunktionalität hat und auf gleichen oder sehr ähnlichen Technologien wie die Originalware basiert [Nee-07 S. 10f.].

Fälschung (auch Falsifikat):
Eine Fälschung bezeichnet ein eigenes Produkt, dem die Urheberschaft eines anderen unterstellt wird [Nee-07 S. 11, in Anlehnung an Bro-12a]. Die Fälschung trägt dabei „ein Zeichen oder anderes Charakteristikum, welches mit einer eingetragenen Marke oder einem Handelsnamen identisch ist. Bei einer Fälschung ist die Täuschung über die Herkunft perfekt ausgeführt. Der Käufer ist der festen Überzeugung, dass er das Produkt eines renommierten Unternehmens erwirbt.“ [Blu-06 S. 34] Dabei kann es sich um eine Fälschung nach Vorbild einer existierenden Originalware handeln oder um Fälschungen, zu denen es keine Originalware gibt [Nee-07 S. 11].

Graumarktware (auch Parallelimport):
Graumarktwaren sind Waren, die für den Vertrieb in Region A bestimmt sind, jedoch in Region B verkauft werden. Kennzeichnend ist, dass „diese Produkte weitestgehend identisch sind und in der Region A günstiger angeboten werden, als in Region B“. [Mei-11 S. 23, Wel-07 S. 24]

Dritte Schicht (auch Overruns, Factory Overruns, Nighttime Production, Mondscheinproduktion):
Waren, die von einem Lizenznehmer über die vom Lizenzgeber genehmigte Anzahl an Produkten hinaus hergestellt und vertrieben werden. [Mei-11 S. 22, Wel-07 S. 25]

Im Zusammenhang mit Marken- und Produktpiraterie im Maschinen- und Anlagenbau ist es insbesondere von Interesse, die in Abbildung 2-2 rot hinterlegten Erscheinungsformen zu bekämpfen. Dies wird in der Literatur unter dem Begriff „Produktschutz“ zusammengefasst:

> **Produktschutz:**
> Im Zusammenhang mit Produkt- und Markenpiraterie ist unter Produktschutz der Schutz der originalen Supply-Chain gegen das Einschleusen von Kopien – insbesondere Piraterieware – in den normalen Warenfluss zum Kunden zu sehen. Dies umfasst ebenso Graumarktware und Waren aus der Dritten Schicht. [Krä-11]

Dass der Produktschutz mit der Kennzeichnung der Originalwaren und deren Authentifizierung zur Abgrenzung von Kopien und gleichermaßen zur Abwehr von Dritte-Schicht- oder Graumarktware gelingen kann, wird in dieser Arbeit dargestellt.

3 Aktueller Stand der Technik

Ausgehend von der Zielformulierung sowie der Darstellung des gewählten Ansatzes zur Zielerreichung in Abschnitt 1.2.2, S. 8 ergibt sich, dass für das technische Produktpiraterie-Schutzsystem zwei wesentliche Komponenten benötigt werden. Einerseits Sicherheitsmerkmale zur Kennzeichnung von Originalbauteilen. Andererseits IP-Punkte zur Authentifizierung der markierten Originale im Wertschöpfungs- und Logistiknetzwerk bis hin zu den Maschinen und Anlagen, die in ihrer Gesamtheit analog zu existierenden Tracking&Tracing-Systemen (T&T-Systeme) funktionieren, aber zusätzlich eine Authentifizierung ermöglichen.

Daher werden in diesem Kapitel neben den Sicherheitsmerkmalen auch existierende Systeme zur Nachverfolgung sowie zur Feststellung der Originalität gesucht und bezüglich der bereitgestellten Funktionalitäten untersucht. Abschließend wird zusammenfassend aufgezeigt, welche Funktionen die einzelnen Technologien und Systeme bieten und welche Lücke demnach im aktuellen Stand der Technik existiert.

3.1 Sicherheitsmerkmale

Im Bereich der Kennzeichnung und Authentifizierung gibt es Schätzungen von Experten zu Folge etwa 300 bis 400 Sicherheitstechnologien, die am Markt verfügbar sind und zum Einsatz kommen [Dir-10, Fuc-12]. Eine vollständige Sammlung oder Übersicht aller derzeit existierenden Technologien gibt es jedoch nicht.

Darüber hinaus ist die Orientierung auf dem Markt der Sicherheitstechnologien für Kunden aus mehreren Gründen zusätzlich erschwert. Zunächst werden die von den Unternehmen angebotenen Sicherheitstechnologien aus Marketinggründen oftmals vollständig umbenannt[9]. Ein Rückschluss auf die hinter einem Produkt stehende Technologie ist damit schwer und ein Vergleich von Produkten sehr schwierig. Darüber hinaus werden – wie bei einem Geldschein – meist Kombinationen von Einzel-

[9] z. B. arbeitet „Lasersecure“ mit Infrarotfarbe, hinter „varifeye“ steckt ein spezielles Foliendurchsichtsfenster und DataDotDNA ist der Markenname für spezielle Mikropunkte (siehe Anhang A.5.4.3.1, A.5.1.1.1 und A.5.4.10)

technologien als ein Produkt dargestellt und am Markt angeboten. Beispielsweise integriert „SecuMed2“ sieben Technologien, unter anderem Kippfarben, geprägte Elemente, holografische Darstellungen und thermochrome Farbe [Sch-13b]. Schließlich gibt es seitens der Hersteller eine nachvollziehbare Zurückhaltung in der öffentlichen Kommunikation, um eine Nachahmung der Sicherheitstechnologien zu erschweren.

In dieser Arbeit wird kein neues Sicherheitsmerkmal entwickelt. Vielmehr wird eine Lösung entwickelt, wie aus den am Markt existierenden Technologien für konkrete Fälle im Maschinen- und Anlagenbau passende Sicherheitsmerkmale ausgewählt und in ein technisches Gesamtsystem integriert werden können.

3.1.1 Katalog existierender Sicherheitsmerkmale

Um dafür eine solide Basis zu haben und um den von Produktpiraterie betroffenen Unternehmen eine Möglichkeit zur schnellen Orientierung im Bereich der Kennzeichnungs- und Authentifizierungstechnologien bereit zu stellen, wird in dieser Arbeit ein neuer, umfangreicher Katalog existierender Sicherheitsmerkmale erstellt. Dabei sind Technologien aufgenommen und gelistet, die prinzipiell für Komponenten und Ersatzteile im Maschinen- und Anlagenbau oder für deren Verpackungen in Frage kommen. Dafür wurden 85 verschiedene Quellen analysiert und dabei 68 verschiedene Technologien herausgearbeitet.

Diese 68 Technologien sollen jedoch nicht einfach nur gelistet, sondern sinnvoll geordnet und gruppiert werden. Dafür wird hier eine neue Struktur zur Klassifizierung der Sicherheitstechnologien aufgrund ihrer Funktionsweise im Authentifizierungsschritt erarbeitet. Diese Funktionsweise ist nicht immer eindeutig zuzuordnen, da oftmals mehrere Details und Eigenschaften eines Sicherheitsmerkmals zusammen die Authentifizierung ermöglichen. In diesem Fall wurde die Zuordnung aufgrund der wichtigsten Funktion für die Authentifizierung vorgenommen. [10]

[10] Das akustomagnetische Etikett beispielsweise wird für die Diebstahlsicherung im Einzelhandel eingesetzt (siehe Anhang A.3.1). Das Etikett wird bei einem Diebstahlversuch durch einen Magentfeldimpuls erkannt und es wird ein optisches oder akustisches Signal ausgelöst [IBH-13]. Dennoch ist das akustomagnetische Etikett aufgrund seiner Funktionsweise in der Klasse „elektrisch / magnetisch / elektromagnetisch“ eingeordnet und nicht aufgrund der ausgelösten Reaktion beispielsweise in „optisch“.

Das Ergebnis ist in Tabelle 3-1 abgebildet. Jede angeführte Technologie hat in der Spalte „Abschnitt“ einen Verweis auf die zugehörige Beschreibung in Anhang A. Dort sind alle gelisteten Technologien dargestellt und die dafür ausgewerteten Quellen angegeben. Zudem sind, sofern verfügbar, Beispiele angeführt und ein aussagekräftiges Bild abgedruckt. Da die ausgewerteten Quellen jeweils lediglich Teilmengen der hier gelisteten und beschriebenen Technologien beinhalten (siehe Quellenangaben in Anhang A) ist dieser Katalog an Sicherheitsmerkmalen und -technologien der aktuell umfangreichste für die produzierende Industrie. Dennoch erhebt der Katalog keinen Anspruch auf Vollständigkeit, da es in diesem Bereich permanent Neuentwicklungen gibt [Bun-13a, EZB-13a].

Tabelle 3-1: Sicherheitsmerkmale

Klasse	Gruppe	Kennzeichen / Technologie / System	Abschnitt
Biologisch	-	Antikörper	A.1.1
		Desoxyribonukleinsäure (DNA)	A.1.2
		DNA-Sequenz	A.1.2.1
		DNA-Strang	A.1.2.2
Chemisch	-	Nanotech Barcode	A.2.1
Elektrisch / magnetisch / elektromagnetisch	-	Akustomagnetisches Etikett	A.3.1
		Elektromagnetisch detektierbare Farbe	A.3.2
		Elektromagnetisches Etikett	A.3.3
		Elektromagnetische Glasfasern	A.3.4
		Mikrochip mit Kontakt	A.3.5
		Radiofrequenzidentifikation (RFID)	A.3.6
Haptisch	**Druckverfahren**	Hochdruck	A.4.1.1
		Matrixdruck / Nadeldruck	A.4.1.2
		Tiefdruck	A.4.1.3
		Intagliodruck / Stichtiefdruck	A.4.1.3.1
		Orlof-Technik / Schabloneneinfärbetechnik	A.4.1.3.2
		Rastertiefdruck	A.4.1.3.3
		Siebdruck	A.4.1.4
	Prägen	Blindprägung	A.4.2.1
		Heißfolienprägung	A.4.2.2

Klasse	Gruppe	Kennzeichen / Technologie / System	Abschnitt
Optisch	Optische Effekte	Durchsichtsfenster	A.5.1.1
		Foliendurchsichtsfenster	A.5.1.1.1
		Moiré Magnifier-Element	A.5.1.1.2
		Durchsichtsregister	A.5.1.2
		Hologramme	A.5.1.3
		Laserkippbild	A.5.1.4
		Parallaxe	A.5.1.5
		Retroreflektierende Folie	A.5.1.6
		Wasserzeichen	A.5.1.7
	Pre-Press-Druckmerkmale	Anti-Kopier-Muster	A.5.2.1
		Besondere Schriftart	A.5.2.2
		Digitale Wasserzeichen	A.5.2.3
		Mikrotext	A.5.2.4
		Rasterbild	A.5.2.5
		Scrambled image / codiertes Bild	A.5.2.6
	Spezialdruck	Guillochen	A.5.3.1
		Irisdruck / Regenbogendruck	A.5.3.2
	Spezialfarben / Spezialpartikel	Clustermerkmal	A.5.4.1
		Fotochrome Farbe	A.5.4.2
		Reversible fotochrome Farbe	A.5.4.2.1
		Irreversible fotochrome Farbe	A.5.4.2.2
		Fluoreszenz	A.5.4.3
		Infrarot-Farbe (IR)	A.5.4.3.1
		Röntgenlumineszenz	A.5.4.3.2
		Tagesleuchtfarbe / Neonfarbe als Echtfarbelement	A.5.4.3.3
		Ultraviolette Farbe (UV)	A.5.4.3.4
		Interferenz- und Effektfarbe	A.5.4.4
		Kippfarbe / optisch variable Druckfarbe	A.5.4.5
		Magnetisierbare Farbe	A.5.4.6
		Metallreagenzfarbe	A.5.4.7
		Metamere Farbe	A.5.4.8
		Mikrofarbcode	A.5.4.9
		Mikropunkte	A.5.4.10
		Pen-Reactive-Ink / Reagenzfarbe	A.5.4.11
		Phosphoreszenz	A.5.4.12
		Sicherheitsfärbemittel	A.5.4.13
		Sonderfarbe	A.5.4.14
		Spektralsensible Farbe	A.5.4.15
		thermoreaktive Farbe	A.5.4.16
		Thermische Pigmente	A.5.4.16.1
		Thermochrome Pigmente	A.5.4.16.2
	Sonstige	Feuchtstempelabdruck	A.5.5.1
		Lasergravur	A.5.5.2
		Oberflächenauthentifizierung	A.5.5.3
		Musteroberfläche	A.5.5.3.1
		Sprengprägen	A.5.5.3.2
		Stochastische Schwankungen im Fertigungsprozess	A.5.5.3.3
		Perforation	A.5.5.4
		Laserperforation	A.5.5.4.1
		Nadelperforation	A.5.5.4.2
		Rauschmustercodes	A.5.5.5
		Sicherheitsanstanzung	A.5.5.6
		Sicherheitsfaden	A.5.5.7
Sonstige	-	Duftstoffe	A.6.1
		Markierung pulvermetallurgisch hergestellter Bauteile	A.6.2
		Nanopartikel	A.6.3

3.1.2 Zusammenfassung Sicherheitsmerkmale

Es gibt eine große Menge an Sicherheitsmerkmalen. Trotzdem ist festzustellen, dass diese „nur“ die Grundfunktionen Echtheitserkennung und Kopierschutz anbieten (siehe Definition in Abschnitt 2.7.1, S. 27). Es wird am Markt also kein Sicherheitsmerkmal angeboten, das in einem Gesamtsystem integriert die Funktion der Authentifizierung mit den Funktionen von T&T-Systemen verknüpft.

Um einen gesamtheitlichen Überblick über den aktuellen Stand der Technik zu erhalten werden die Ergebnisse aus diesem Kapitel im Abschnitt 3.4 zusammengefasst. Dort erfolgt auf S. 71 in Tabelle 3-3 in der Zeile „3.1 Sicherheitsmerkmale“ aufgrund der angeführten Erkenntnisse der Eintrag, dass die Authentifizierung unter Verwendung von Sicherheitsmerkmalen erfolgen kann, aber kein T&T oder ein technisch integriertes Gesamtsystem angeboten wird. Auch die Erkenntnisse aus den nächsten Abschnitten werden jeweils in diese zusammenfassende Übersicht eingetragen.

3.2 Existierende Systeme zur Nachverfolgung und zur Feststellung der Originalität

Da in dieser Arbeit die Möglichkeiten des T&T kombiniert werden sollen mit der Funktion der Authentifizierung, werden T&T-Systeme zunächst eingeführt und der Stand der Technik bei diesen Systemen beschrieben. Dabei wird auch festgestellt, welche Funktionen aktuelle T&T-Systeme bereits implementieren. Anschließend werden existierende Systeme daraufhin untersucht, ob diese neben T&T auch die Funktion der Authentifizierung auf Basis von Sicherheitsmerkmalen integrieren.

3.2.1 Tracking&Tracing-Systeme allgemein

T&T-Systeme sind als Nachverfolgungssysteme in der Logistik bereits vielfach anzutreffen und wie folgt beschrieben:

Tracking&Tracing-System (T&T-System):
Tracking&Tracing ist ein in der Logistik häufig verwendetes, computergestütztes, innerbetriebliches wie auch außerbetriebliches Konzept zur Sendungsverfolgung und beinhaltet zwei Aspekte. Das „Tracking“ verfolgt logistische Einheiten auf ihrem Weg durch die Supply-Chain und stellt den aktuellen Status dieser logistischen Einheit fest. Unter „Tracing“ wird dagegen die Rückverfolgung, also das Nachvollziehen der Herkunft einer logistischen Einheit verstanden. Kernpunkt von T&T-Systemen ist damit die Schaffung einer durchgängigen Transparenz innerhalb der logistischen Ketten. Hierfür werden spezielle Softwareanwendungen eingesetzt, welche die Daten via Internet zur Verfügung stellen und aufbereiten. [Arn-08 S. B 8-17, Bre-02 S. 3, Hom-06]

T&T-Systeme implementieren die folgenden drei Prozessschritte [Bre-02 S. 10 ff.]:

- Identifikation und Datenerfassung (siehe Abschnitt 3.2.1.1)
- Datenübertragung (siehe Abschnitt 3.2.1.2)
- Datenverarbeitung und -aufbereitung (siehe Abschnitt 3.2.1.3)

Dafür erhält jede logistische Einheit ein elektronisch lesbares Etikett, das alle transportrelevanten Informationen enthält (z. B. Barcode, RFID-Transponder). Bei jedem transportrelevanten Schritt (z. B. Warenausgang, Wareneingang, Verladung, Entladung) wird das Etikett an einem Identifikationspunkt (siehe Definition) erfasst und die Identität, etwaige transportrelevante Informationen sowie Orts- und Zeitangabe an das zugehörige Datenarchivierungs- und -auswertesystem gesendet (siehe Abbildung 3-1). Durch die Auswertung aller Informationen zu einer logistischen Einheit lässt sich die aktuelle Position bestimmen und ein Überblick über den zeitlichen und örtlichen Verlauf des Transportes generieren. [Arn-08 S. B 8-17, Bre-02]

Identifikationspunkt (I-Punkt):
Ein I-Punkt ist ein Ort in der Supply-Chain, an dem logistische Einheiten mittels elektronisch lesbarer Etiketten identifiziert werden. Die Identiät und etwaige beinhaltete transportrelevante Informationen werden zusammen mit Orts- und Zeitangabe an das zugehörige Datenarchivierungs- und -auswertesystem weitergeleitet. [Arn-08 S. B 8-17, Bre-02 S. 12 ff.]

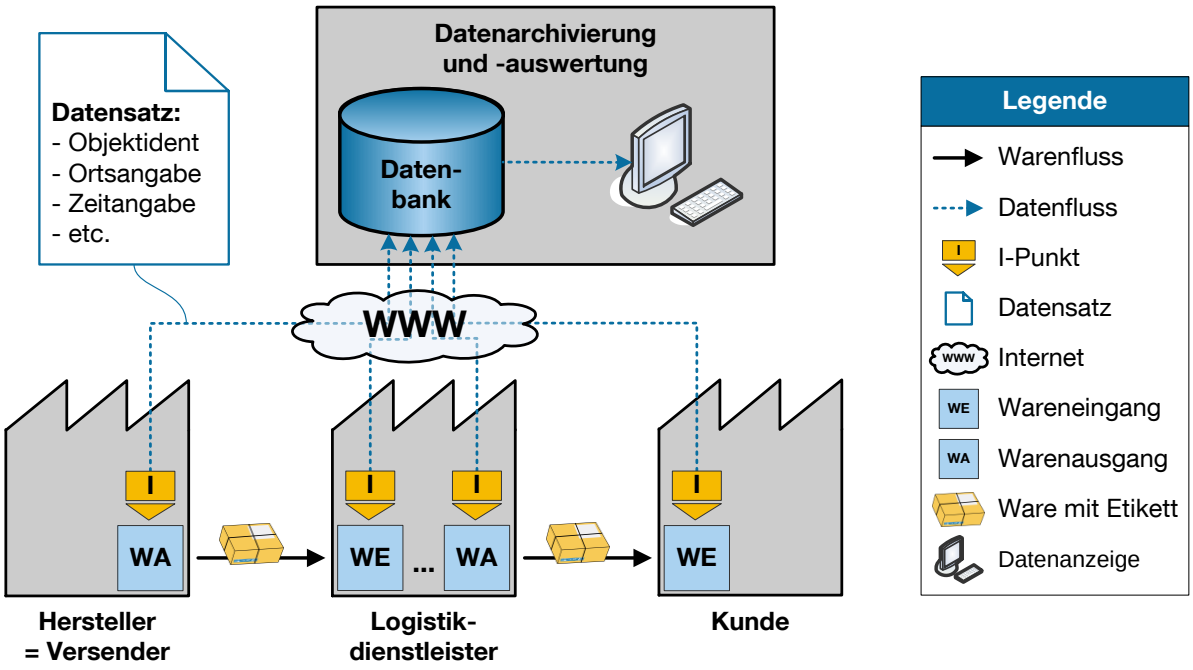


Abbildung 3-1: Schematische Darstellung eines Tracking&Tracing-Systems[11]

Da für die einzelnen Funktionen in T&T-Systemen verschiedene Konzepte und Technologien zum Einsatz kommen können, haben *Bretzke et al.* acht Kriterien zur Charakterisierung von T&T-Systemen erarbeitet [Bre-02 S. 3]. Diese Kriterien zeigen gleichzeitig die Bandbreite existierender technischer Lösungen für T&T-Systeme auf und sind in Abbildung 3-2 zusammengefasst.

[11] Die Darstellung erfolgte in Anlehnung an Bretzke et al. [Bre-02 S. 25] und das von Gudehus vorgeschlagene Strukturdiagramm [Gud-12 S. 82] und wurde mit IT-Entitäten der UML - Unified Modeling Language [Rup-07 S. 223] ergänzt. Inhalte stammen aus den Quellen Arn-08 S. B 8-17, Bru-13 S. 17, Gün-06a S. 36, Gün-12a S. 28 f., Org-13 S. 6 sowie Tre-13 S. 8.

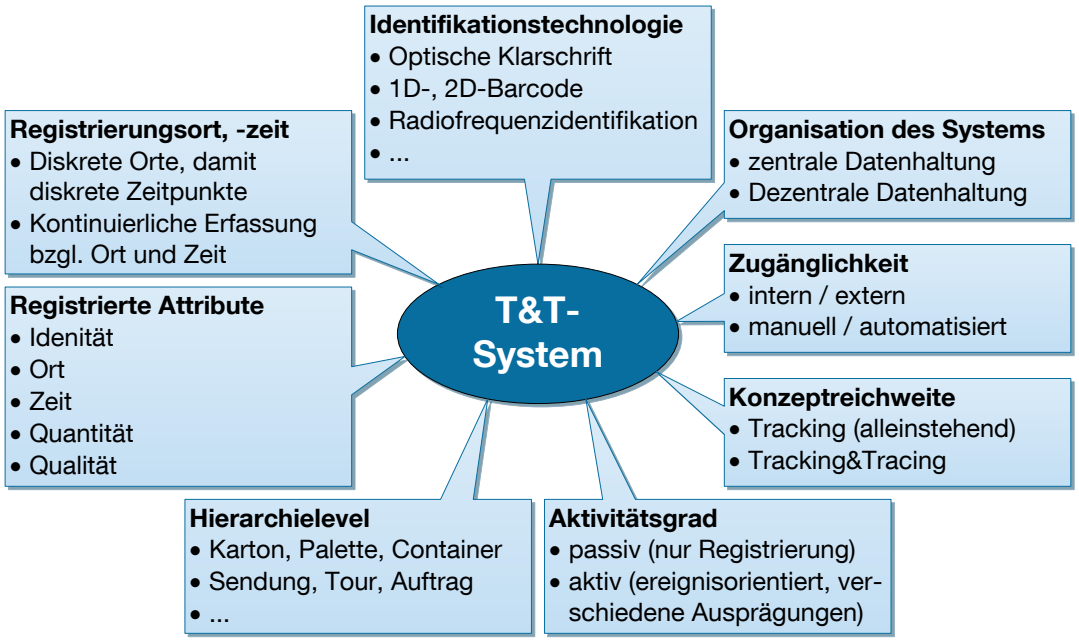


Abbildung 3-2: Funktionen in und gleichzeitig Kriterien zur Beschreibung von T&T-Systemen, nach [Bre-02 S. 3]

3.2.1.1 Identifikation und Datenerfassung

Zur Identifikation von logistischen Einheiten in einer Supply-Chain werden diese mit elektronisch lesbaren Etiketten ausgestattet. Dabei können unterschiedliche Technologien zum Einsatz kommen (siehe Abbildung 3-3). Die in Etiketten enthaltenen Daten können an einem stationären oder mobilen I-Punkt automatisch oder manuell erfasst und in das T&T-System übertragen werden [Bre-02 S. 12 ff.]. Der schematische Aufbau eines solchen Identifikationssystems ist der VDI-Richtlinie 4416 entnommen und mit zwei gängigen Beispielen ergänzt in Abbildung 3-4 dargestellt.

Um das korrekte Auslesen und Interpretieren der Daten eines Etiketts auch unternehmensübergreifend zu gewährleisten, gibt es verschiedene Standards, die für die jeweiligen Identitätskennzeichen zum Einsatz kommen.[12] Die Standards des internationalen Standardisierungsdienstleisters Global Standards One (GS1) zählen dabei zu den bekanntesten unternehmensübergreifenden Symbolik- und Anwendungsstandards. Sie sind aus den UCC- / EAN-Standards hervorgegangen und mittlerweile weltweit verbreitet [Bre-02 S. 14, Fin-12 S. 368, GS1-13a].

[12] Übersicht für Barcodes: siehe [Bar-11, Bre-02 S. 14, Dat-07, GS1-13c], Übersicht für RFID: siehe [Fin-12 S. 303, Kov-12]

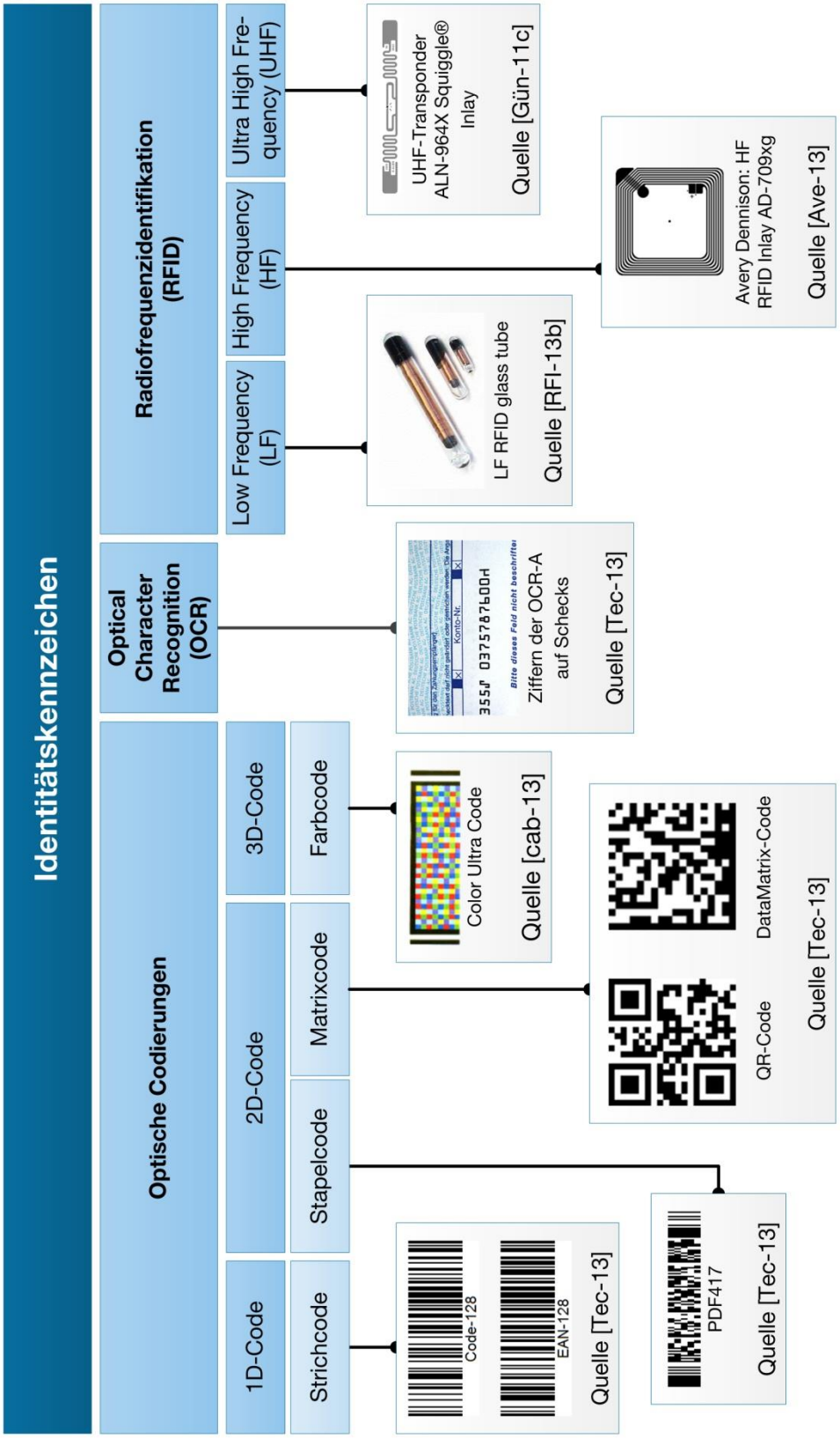


Abbildung 3-3: Wesentliche maschinenlesbare Identitätskennzeichen, in Anlehnung an [Fin-12, Dat-07, Bar-11]

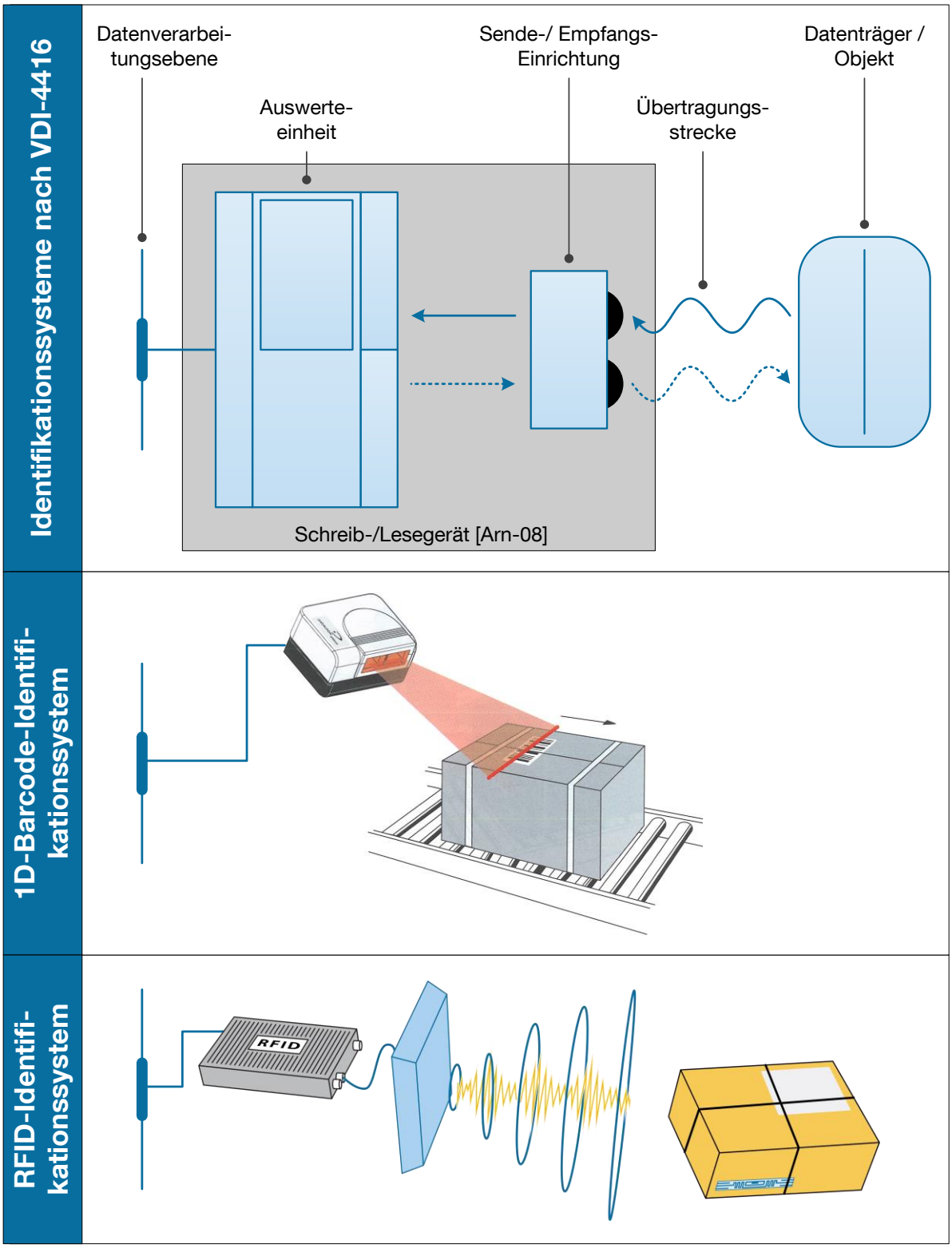


Abbildung 3-4: **Identifikationssysteme zur Identifikation einer logistischen Einheit an einem I-Punkt: schematisch nach VDI-4416 sowie in Realisierung als 1D-Barcode bzw. RFID-System [VDI4416, Dat-07, fml-13c]**

Grundvoraussetzung für die Einrichtung eines funktionierenden T&T-Systems ist die Individualisierung der logistischen Einheiten mit Hilfe von Identitätskennzeichen (siehe Abbildung 3-3). Dafür werden beispielsweise fortlaufende Nummern vergeben

[Glo-06 S. 176, Wil-07 S. 67, S. 72 f.]. Dabei ist wichtig, dass diese Nummern weltweit überschneidungsfrei erzeugt und vergeben werden, so dass kein Identitätskennzeichen mehrmals existiert. Dies kann beispielsweise mit dem Nummernsystem der GS1 erreicht werden. Dabei erhält jedes teilnehmende Unternehmen einen eigenen, weltweit einmaligen Code, das sogenannte „Company Prefix“. Damit ist dieses Unternehmen berechtigt, Sachnummern und Seriennummern für Objekte gemäß der Systematik und Standards der GS1 zu vergeben [GS1-13c S. 18]. Das Vorschalten des Company Prefix vor die, durch das jeweilige Unternehmen vergebenen Sach- und Seriennummern macht den gesamten erzeugten Code einmalig und ist von allen Wirtschaftsbeteiligten in der Repräsentanz eines Barcodes oder auch gespeichert in einem RFID-Transponder les- und interpretierbar.

Eine Übersicht über die verschiedenen durch GS1 definierten Codes sowie deren Aufbau ist in Anhang B gegeben. Als Beispiel wird die Serialized Global Trade Item Number (SGTIN) herausgegriffen, die dem beschriebenen Aufbau aus Company Prefix, Sachnummer und Seriennummer folgt (siehe Abbildung 3-5). Die SGTIN ist eine Weiterentwicklung der Europäischen Artikelnummer EAN [Glo-06 S. 83] und für die Kennzeichnung einzelner Produkte gedacht [GS1-13b S. 29].

Serialized Global Trade Item Number (SGTIN)		
Company Prefix	**Sachnummer**	**Seriennummer**
Dezimal (7-stellig): 4290039 Binär (24 Bit): 01000001 01110101 11110111	Dezimal (6-stellig): 687246 Binär (20 Bit): 1010 01111100 10001110	Dezimal (12-stellig): 000000000045 Binär (38 Bit): 000000 00000000 00000000 00000000 00101101
Dezimal (25-stellig): 4290039 687246 000000000045 Binär (82 Bit): 01 00000101 11010111 11011110 10011111 00100011 10000000 00000000 00000000 00000000 00101101		

Abbildung 3-5: Aufbau der Serialized Global Trade Item Number (SGTIN) an einem Beispiel, nach [GS1-13b]

3.2.1.2 Datenübertragung

Nachdem eine logistische Einheit an einem I-Punkt erfasst wurde, müssen die T&T-Daten den am Informationsfluss beteiligten Partnern in der Supply-Chain zur Verfügung gestellt werden [Bre-02 S. 19]. Dabei kann der unternehmensübergreifende Datenaustausch mittels strukturierter Daten automatisch erfolgen – dies wird als

Electronic Data Interchange (EDI) bezeichnet [Bre-02 S. 19, Hom-06]. Zwar sind die meisten EDI-Verbindungen bilateral zwischen zwei Unternehmen, aber auch im Bereich der elektronischen Datenübertragung schreitet die Standardisierung stetig voran [Bre-02 S. 19]. Dabei werden verschiedene Datenübertragungswege genutzt: innerbetrieblich Local Area Network (LAN) und Wireless LAN (WLAN), überbetrieblich Internet und bei mobilen Lösungen das Global System of Mobile Communication (GSM) [Bre-02 S. 19 f.].

Der einzige bisher weltweit anerkannte EDI-Standard ist der „Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)“ [Bre-02 S. 20], der in der DIN ISO 9735 beschrieben und veröffentlicht ist [DIN9735 1-10]. Die innerhalb des Standards definierten EDIFACT-Nachrichten wurden für verschiedene Branchen in Subsets geclustert. Im Logistikbereich heißt dieses Subset EANCOM[13], das speziell für den Informationsaustausch zwischen Hersteller- und Handelsinformationssystemen im Konsumgüterbereich geschaffen wurde [Bre-02 S. 21]. Für den Anwendungsbereich T&T ist EANCOM deshalb von großer Bedeutung [Bre-02 S. 21].

Eine Weiterentwicklung der Nachrichtenübermittlung erfolgt durch die Verwendung der Auszeichnungssprache XML (Extensible Markup Language), die sehr gut für die Übertragung strukturierter Informationen geeignet ist. Regeln zur Generierung von XML-Schemadateien aus EDI(FACT)-Anwendungsbeschreibungen sind in der DIN 16557-5 festgehalten [Bre-02 S. 22, DIN16557-5]. Der in Abbildung 3-1 dargestellte Datensatz kann somit insbesondere auch als XML-Nachricht zur Verfügung gestellt oder versendet werden. Ein Beispiel für eine XML-Nachricht zur Darstellung ihrer Struktur ist in Abbildung 3-6 zu sehen.

[13] EANCOM ist ein Kunstwort aus EAN und Communication, siehe [Hom-06]

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- automatically generated by GEFEG EDIFIX -->
<!-- http://www.gefeg.com -->

<Bestellung xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="orders-speaking-ohneNS.xsd">
     <Bestellnummer>1-96</Bestellnummer>
     <Bestelldatum>19960101</Bestelldatum>
     <Lieferdatum>19960110</Lieferdatum>
     <Kaeufer>
          <Kaeufer_Adresse>
               <KaeuferName>BONBON AG</KaeuferName>
               <KaeuferStrasse>SIRUPSTRASSE 15</KaeuferStrasse>
               <KaeuferOrt>ZUCKERSTADT</KaeuferOrt>
               <KaeuferPostleitzahl>55555</KaeuferPostleitzahl>
          </Kaeufer_Adresse>
          <KaeuferBankverbindung>
               <KaeuferKontonummer>1236547890</KaeuferKontonummer>
               <KaeuferBankleitzahl>10090045</KaeuferBankleitzahl>
               <KaeuferBankname>SBANK</KaeuferBankname>
          </KaeuferBankverbindung>
          <USt-IDNr>DE9988877</USt-IDNr>
          <KaeuferAnsprechpartner>Bart Simpson</KaeuferAnsprechpartner>
          <KaeuferTelefonnummer>05368-22347</KaeuferTelefonnummer>
          <KaeuferFaxnummer>05368-22555</KaeuferFaxnummer>
     </Kaeufer>
     <Verkaeufer>
          <Verkaeufer_Adresse>
               <VerkaeuferName>KAKAO GMBH</VerkaeuferName>
               <VerkaeuferStrasse>FRUCHTSTRASSE 1</VerkaeuferStrasse>
               <VerkaeuferOrt>SAHNEBERG</VerkaeuferOrt>
               <VerkaeuferPostleitzahl>98765</VerkaeuferPostleitzahl>
          </Verkaeufer_Adresse>
     </Verkaeufer>
     <Bestellwaehrung>EUR</Bestellwaehrung>
     <Positionsdaten>
          <Positionsnummer>1</Positionsnummer>
          <Artikelnummer>2001</Artikelnummer>
          <Artikelbeschreibung>
               <Artikeltext1>SCHOKOLADENMASSE</Artikeltext1>
               <Artikeltext2>BRAUN</Artikeltext2>
          </Artikelbeschreibung>
          <Bestellmenge>2</Bestellmenge>
          <Masseinheit>TNE</Masseinheit>
          <Positionspreis>2800</Positionspreis>
          <Einzelpreis>1400</Einzelpreis>
     </Positionsdaten>
     <Bestellwert>2800</Bestellwert>
</Bestellung>
```

Abbildung 3-6: Darstellung einer Bestellung im XML-Schema nach DIN 16557-5 [DIN16557-5 S. 57]

3.2.1.3 Datenverarbeitung und -aufbereitung

Nach der Übermittlung der T&T-Daten werden diese in Datenbanksystemen verwaltet und stehen damit strukturiert zur Verfügung. Datenbanksysteme können zentral oder verteilt organisiert sein. [Bre-02 S. 25, Hom-06]

Die Auswertung macht aus Informationen für die Teilnehmer des T&T-Systems wertvolles Wissen, wie z. B. der Soll-Ist-Abgleich eines Auslieferungsplans [Bre-02 S. 25] (siehe Abbildung 3-7). Denn „nur ein durchgehender und unternehmensübergreifender Informationsfluss ermöglicht es, wichtige Informationen aus komplexen Prozessen herauszufiltern, die Informationsbarrieren, die zu Intransparenz führen, zu durchdringen und zeitnah im Sinne von dynamisch auf ein auftretendes Problem zu reagieren.“ [Bre-02 S. 29]

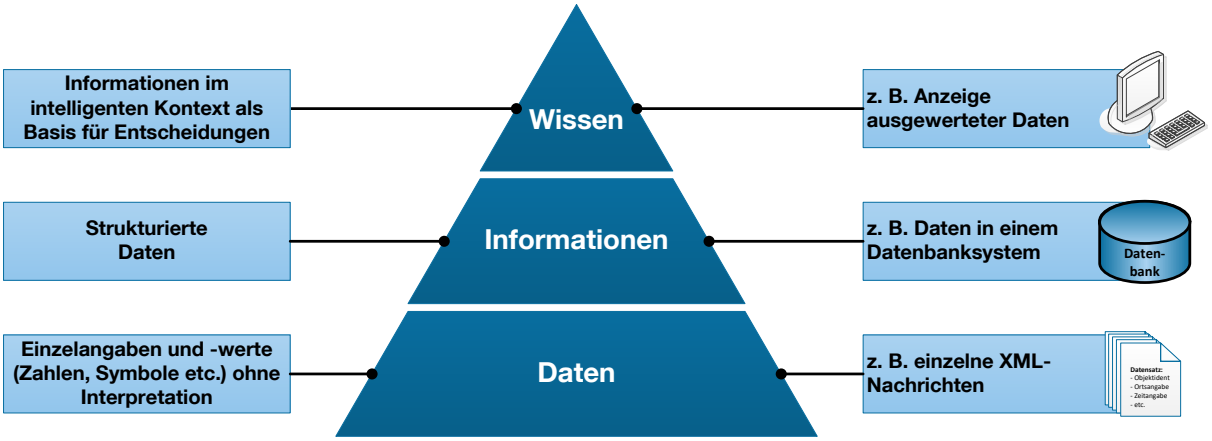


Abbildung 3-7: Wissenspyramide [Cha-05 S. 224], erweitert um Beispiele aus einem T&T-System (siehe Abbildung 3-1)

Die gesammelten Daten sollen jedoch nicht jedem Beteiligten gleichermaßen vollständig zur Verfügung stehen. Insofern ist innerhalb von T&T-Systemen festzulegen, welche Daten welchem Personenkreis zugänglich gemacht werden [Bre-02 S. 26]. Dies kann durch eine rollenbasierte Zugriffskontrolle (RBAC: Role Based Access Control) erreicht werden, wie diese durch *Ferraiolo und Kuhn* bereits 1992 konzeptionell entwickelt [Fer-92] und seither vielfach in verschiedensten Softwarelösungen implementiert wurde [NIST-13].

Neben dem Rollenkonzept zur Regelung des Zugriffs auf die gesammelten Daten muss auch die Datenübertragung sowie die Archivierung und Auswertung der Daten vor unbefugtem Zugriff durch Dritte geschützt werden. Auch in diesem Bereich gibt es passende Maßnahmen, um sämtliche Kommunikation sowie die Daten selbst zu schützen [Bre-02 S. 26]. Der Schutz der Kommunikation kann mittels des Secure

Socket Layer-Protokolls (SSL) oder mit dessen aktuellster Weiterentwicklung dem Transport Layer Security-Protokoll (TLS) erfolgen [Bre-02 S. 26, Neu-11, Sch-10b S. 83]. Der Schutz der Daten in einem zentralen oder verteilten Datenbanksystem, dessen Anbindung an das Internet zur sinnvollen Einbindung in das T&T-System und zur Nutzung innerhalb des T&T-Systems notwendig ist, ist jedoch ohne Sicherheits-Gateway (auch: Firewall) undenkbar. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich seit vielen Jahren mit diesem Thema und stellt zahlreiche Veröffentlichungen dazu zur Verfügung [BSI-13b, siehe auch BSI-13c].

3.2.1.4 Zusammenfassung Tracking&Tracing-Systeme allgemein

T&T-Systeme dienen der Verfolgung und Rückverfolgung von Objekten in der Supply-Chain und bieten keine Authentifikation der Objekte an (siehe Abbildung 3-2). Somit können in der Übersicht in Tabelle 3-3, S. 71 in der Zeile „3.2.1 Tracking&Tracing-Systeme allgemein“ die entsprechenden Eintragungen vorgenommen werden.

Ursprünglich wurden T&T-Systeme von Kurier-, Express-, und Paketdiensten (KEP) genutzt, um die Auskunftsfähigkeit gegenüber Kunden zu erhöhen; in diesem Teilbereich der Logistik gehört T&T bereits zum Stand der Technik [Arn-08 S. B 8-17]. Daher wird das für T&T-Systeme allgemein gewonnene Ergebnis an einem konkreten Beispiel eines Logistikdienstleisters bestätigt.

3.2.2 Tracking&Tracing bei KEP-Diensten

Als schon beinahe klassisches Beispiel wird hier das T&T-System des Logistikdienstleisters DHL untersucht. Die in Bonn ansässige DHL GmbH ist Weltmarktführer bei Luft- und Seefracht, weltweit das umsatzstärkste Logistikunternehmen [Mac-10, Gat-13] und bietet für seine Kunden ein T&T-System an. Abhängig der zu transportierenden Güter unterscheiden sich die Serviceumfänge, die den Kunden zur Verfügung stehen. Das System „Active Tracing“ beispielsweise ermöglicht eine vollständige Transparenz für aufgegebene Straßenfrachten (siehe Abbildung 3-8) und beinhaltet folgende Funktionen [Deu-13c]:

- Zugang zu allen aktuellen Sendungsinformationen für registrierte Kunden
- Sendungshistorie mit Scandaten von Abholung bis Auslieferung für den Zeitraum von bis zu sechs Monaten

- Umfassende Sendungsdaten zu wichtigen Zwischenzielen
- Papierloser Informationsfluss

Als T&T-System, das vollständig der Definition entspricht (siehe S. 42), bietet dieses System keine Möglichkeit an, Sendungen als integrierte Funktion anhand von Sicherheitsmerkmalen zu authentifizieren. Daher erfolgen in der Übersicht in Tabelle 3-3 auf S. 71 in der Zeile „3.2.2 Tracking&Tracing bei KEP-Diensten“ die entsprechenden Einträge.

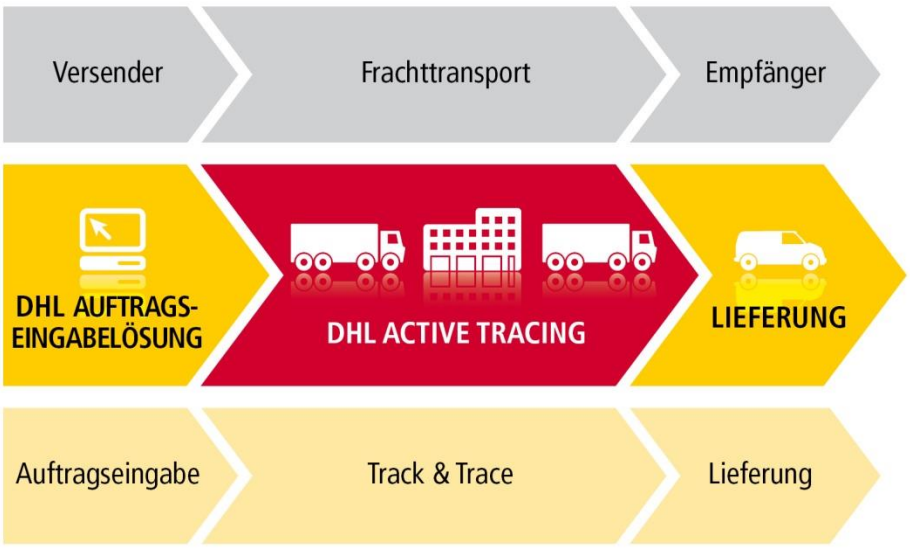


Abbildung 3-8: Tracking&Tracing-System von Deutsche Post DHL [Deu-13c]

3.2.3 Tracking&Tracing in der Luft- und Raumfahrtbranche

Dass T&T-Systeme der Logistikdienstleister die Funktionalität der Authentifizierung auf Basis von Sicherheitsmerkmalen nicht anbieten, ist nicht weiter verwunderlich. Daher wird als nächstes das T&T in der Luft- und Raumfahrtbranche untersucht. Dafür wurde ein Expertengespräch geführt [Ric-08], aus dem die folgenden Inhalte stammen.

Richter erläutert, dass in der Luft- und Raumfahrt eine Rückverfolgbarkeit für Bauteile abhängig von deren Einstufung behördlich vorgeschrieben ist. Dabei gibt es drei Klassen:

- Klasse 1:
  Versagen des Bauteils führt direkt zum Absturz des Fluggerätes
- Klasse 2:
  Funktionsstörung, aber das Fluggerät bleibt bis zur Landung flugfähig

- Klasse 3:
  Versagen des Bauteils verursacht meist nur wirtschaftliche Schäden und hat keine schweren Auswirkungen (z. B. nur erhöhter Spritverbrauch)

Für die Bauteile der Klasse 1 und 2 wird eine Rückverfolgbarkeit von der Schmelze bis zur Verschrottung verlangt. Die zugehörigen Daten müssen für 40 Jahre einsehbar sein. Dies wird durch Zertifizierung der US-Luftfahrtaufsichtsbehörde (FAA: Federal Aviation Administration) und der Europäischen Agentur für Flugsicherheit (EASA: European Aviation Safety Agency) in den einzelnen Unternehmen wiederholend überprüft. Nur zertifizierte Unternehmen dürfen Bauteile aller Klassen herstellen und diese mit einem Zertifikat versehen. Bauteile der Klasse 1 oder 2 werden zusätzlich durch entsprechende Codes individualisiert. Diese Codes setzen sich zusammen aus:

1. Sachnummer: Lässt Rückschluss auf Konstruktionszeichnung zu
2. Herstellercode: von der Organisation des Nordatlantikvertrags (NATO: North Atlantic Treaty Organization) oder dem Dachverband amerikanischer Fluggesellschaften (ATA: Air Transport Association) vergebener Code, der den vertraglichen Hersteller des Bauteils anzeigt.
3. Suppliercode: von NATO oder ATA vergebener Code, der den physischen Hersteller des Bauteils anzeigt.
4. Serialnummer: Nummer, die der Hersteller vergibt und die das Bauteil zum Unikat macht
5. Heat Code Suffix: Nummer, die den Rückschluss auf den Hersteller des Gussteils, die Meisterschmelze, die Blocklage in der Bramme und den Schmied ermöglicht

Diese Nummern und Codes müssen in Klarschrift auf den Bauteilen der Klasse 1 und 2 angebracht werden und die gesamte Lebensdauer des Bauteils überdauern. Bei der Kennzeichnung der Bauteile sind folgende Technologien im Einsatz:

- Schlagpunkte zur Erzeugung einer Schrift (ca. 0,1 mm Tiefe)
- Vibrogravieren (ca. 0,1 mm Tiefe)
- Elektrochemisches Ätzen (ca. 0,003 mm Tiefe)
- Laserkennzeichnen (ca. 0,008 mm Tiefe)

Zeitgleich zur Kennzeichnung der Bauteile erfolgt ein Datenbankeintrag, der beim Einbau eines Bauteils in ein Fluggerät überprüft wird. Anhand der Kombination

Sachnummer, Herstellercode und Serialnummer wird das Bauteil eindeutig identifiziert und mittels Datenbankabgleich als Original bestätigt. Bei nicht-bestätigten Codes oder einer Mehrfachvergabe wird das entsprechende Bauteil vertieft geprüft oder direkt aussortiert.

Alle aussortierten Teile – sei es aufgrund unbestätigter Herkunft oder aufgrund des Erreichens der maximalen Lebensdauer – werden von zertifizierten Verschrottungsunternehmen entsorgt. So gelangen keine Nummern von bereits aussortierten Teilen erneut in die Bauteil- und Ersatzteillieferkette. [Ric-08]

Mit diesen Ausführungen ist klar, dass die Authentifizierung von Bauteilen in der Luft- und Raumfahrtbranche auf Basis der Nummernsystematik und eines Datenbankabgleichs erfolgt, also insbesondere nicht auf Basis von Sicherheitsmerkmalen. Auch hier erfolgt der entsprechende Eintrag in der zusammenfassenden Tabelle 3-3 auf S. 71 in der Zeile „3.2.3 Tracking&Tracing in der Luft- und Raumfahrtbranche“.

3.2.4 Software zur Authentifizierung von Produkten und Dokumenten

Bei der Recherche weiterer Lösungen, die ein T&T und eine Authentifizierung auf Basis von Sicherheitsmerkmalen in einem technischen System integrieren, ist festzustellen, dass es lediglich ein System gibt, das dieser Funktionalität nahe kommt.

„Original 1“ war ein Joint-Venture von Giesecke & Devrient, Nokia und SAP. Im Oktober 2009 gegründet war es das Ziel des Unternehmens, „einen weltweit nutzbaren Dienst zur Bekämpfung von Produktpiraterie in unterschiedlichen Branchen bereitzustellen“. Dabei wurden Produkte mit zweidimensionalen Barcodes versehen und an verschiedenen Stellen der Lieferkette dadurch authentifiziert, dass die Barcodes mit einem Mobiltelefon erfasst und die gelesene Produktinformation online mit einer Datenbank abgeglichen wurden. Das System kombinierte die Logistik-Lösung von SAP und die mobile Authentifizierung von Nokia und wurde für Dritte als Software-as-a-Service angeboten. Später sollte „der Dienst auf die Erkennung und Verfolgung von herkömmlichen Barcodes, RFIDChips und Hologrammen ausgedehnt werden.“ [Mar-09]

Dieses Joint-Venture wurde im Jahr 2013 aufgelöst, das System jedoch wird in ähnlicher Form von Giesecke & Devrient weitergeführt [Gie-13c]. Das Unternehmen Giesecke & Devrient bietet demnach eine weltweit nutzbare Software zur Authentifizierung von Produkten und Dokumenten an. Gemäß den Angaben aus einer Exper-

tenbefragung (siehe [Pau-13]) werden im Folgenden die Funktionen dieses Systems dargestellt.

Die als Originale zu kennzeichnenden Produkte bzw. Dokumente werden mit einem serialisierten 2D-Barcode versehen. Bei einem Scan dieses 2D-Barcodes mittels einer proprietären App erhält der berechtigte Nutzer aus einer sicheren Datenbank Auskünfte über das vorliegende Objekt. Durch das implementierte T&T-System kann der berechtigte Prüfer in Echtzeit den Weg des Objektes im Detail einsehen und aufgrund der Produkthistorie eine Plausibilitätsprüfung durchführen. Zudem wird dem Nutzer mitgeteilt, welche weiteren Sicherheitsmerkmale in welcher Form und Ausprägung auf dem vorliegenden Objekt vorhanden sein müssen. Die manuelle Prüfung dieser Sicherheitsmerkmale ermöglicht eine zweifelsfreie Authentifizierung des Objektes. Schließlich kann durch das System eine Warnung erfolgen, sofern 2D-Barcodes respektive Objekte mehrfach geprüft wurden. [Pau-13]

Dieses System einer mobilen Authentifizierung ist eine von Giesecke & Devrient angebotene Komplettlösung. Ein Kunde kann aus angebotenen Sicherheitsmerkmalen wählen und wird dabei von den Experten des Unternehmens unterstützt. Diese Lösung kann auch wie in Abschnitt 3.3.3 bei Arzneimitteln zum Einsatz kommen. Die 2D-Barcodes werden dabei zur Individualisierung der Medikamente im Verpackungsprozess aufgebracht und anschließend einer automatischen 100%-Prüfung bezüglich der Funktionsfähigkeit des neuen Codes unterzogen. [Pau-13]

Die in diesem Abschnitt vorgestellte Software zur Authentifizierung von Produkten und Dokumenten geht somit einen Schritt weiter. Die Authentifizierung erfolgt im ersten Schritt wie beim Tracking&Tracing in der Luft- und Raumfahrtbranche (siehe Abschnitt 3.2.3) ebenfalls über einen Datenbankabgleich, wobei die Zeichenfolge in einem serialisierten 2D-Barcode repräsentiert ist. Dieser kann jedoch nicht zu den Sicherheitsmerkmalen gezählt werden und ist nicht gegen Fälschung sicher. Im zweiten Schritt wird der Benutzer mittels des implementierten T&T-Systems über Sicherheitsmerkmale informiert, welche am Originalprodukt angebracht sind. Die Überprüfung dieser Merkmale soll es dem Nutzer ermöglichen, Produkte oder auch Dokumente als Originale zu bestätigen. Dieser manuelle Authentifizierungsschritt findet außerhalb des technischen Systems statt. Damit liegt das Prüfergebnis lediglich kurzfristig dem jeweiligen Nutzer vor, das Prüfergebnis wird nicht systemseitig erfasst oder dokumentiert. Zudem gibt es für dieses System aktuell keine Realisierungen im Maschinen- und Anlagenbau. Darüber hinaus handelt es sich um ein

proprietäres System der Firma Giesecke & Devrient und ist nicht offen oder allgemeingültig implementiert. Daher werden für dieses System in der Übersicht in Tabelle 3-3, S. 71 in der Zeile „3.2.4 Software zur Authentifizierung von Produkten und Dokumenten“ ebenfalls die entsprechenden Eintragungen vorgenommen.

3.2.5 Zusammenfassung Tracking&Tracing-Systeme

Über die aufgeführten Systeme hinaus gibt es derzeit kein System, das, wie in Abschnitt 1.2.2, S. 8 formuliert, eine Authentifizierung von Originalwaren auf Basis von Sicherheitsmerkmalen mit den Funktionen von Tracking&Tracing-Systemen kombiniert und in einem technischen Produktpiraterie-Schutzsystem integriert. Daher wird der Fokus im folgenden Abschnitt über designierte T&T-Systeme hinaus erweitert.

3.3 Existierende Systeme zur Sicherstellung der Originalität

3.3.1 Originalität einer Tintenpatrone

Ein Beispiel, das im Zusammenhang mit dem Komponentenverkauf im After-Sales nahezu immer genannt wird, ist der Consumerbereich von Drucksystemen. Daher werden die Maßnahmen, welche die Originalhersteller ergriffen haben, um sich ihre Marktanteile zu sichern, genau untersucht.

Im Consumerbereich von Drucksystemen übersteigen insbesondere bei Tintenstrahlgeräten die Kosten für Verbrauchsmaterialien (ohne Papier und elektrischen Strom) die Anschaffungskosten auch bei geringen Druckumfängen von ca. 20 Seiten pro Monat meist bereits in den ersten beiden Jahren [Röß-13]. Vergleichbar zum Maschinen- und Anlagenbau versuchen die Kunden auch hier Betriebskosten zu senken, indem sie alternative Verbrauchsmaterialien von Konkurrenzanbietern einsetzen. Denn beim „Einsatz von Alternativtinte lässt sich […] fast zum Nulltarif drucken“ [Ger-07]. Dabei werden auf dem Markt drei Möglichkeiten angeboten [Ger-07, Ger-09]:

- Komplettnachbau einer Tintenpatrone
- wieder befüllte Original-Tintenpatronen
- Tinten zum Nachfüllen in eigene vorhandene Tintenpatronen

Die Originalhersteller reagieren auf den so entstehenden Wettbewerb mit sehr unterschiedlichen Strategien. Ansatzpunkt der Originalhersteller ist dabei die Überwachung des Füllstands der Patronen.[14]

Im Consumerbereich von Drucksystemen ist die Situation also ähnlich zum Maschinen- und Anlagenbau: Das Geschäft mit Verbrauchsmaterialien ist besonders lukrativ und lockt viele Wettbewerber. Die Reaktionen der Hersteller darauf sind sehr unterschiedlich, wie *Gerber und Labusga* feststellen [Ger-09]. Da dies die einzige auffindbare Quelle mit detaillierten Inhalten ist, wird diese in den nächsten Unterabschnitten mehrfach zitiert, um die Strategien der Originalhersteller im Consumerbereich von Drucksystemen detailliert darstellen zu können.

Wie in diesen Ausführungen deutlich werden wird, aber bereits aus der zusammenfassenden Übersicht in Tabelle 3-2 hervorgeht, gibt es auch bei Drucksystemen des Consumerbereichs kein System, wie es in der vorliegenden Arbeit entwickelt wird. Weder erfolgt eine Authentifizierung eingesetzter Tintenpatronen, noch werden Sicherheitsmerkmale auf den Original-Patronen eingesetzt. Daher erfolgen im Vorgriff auf die detaillierte Analyse die entsprechenden Einträge in der zusammenfassenden Tabelle 3-3, S. 71 in den Zeilen zu „3.3.1 Originalität einer Tintenpatrone“.

[14] Denn bei längerem Drucken ohne Tinte brennen die Düsen durch und der entstandene Schaden ist meist gleichbedeutend mit einem ökonomischen Totalschaden des Druckers [Ger-08].

Tabelle 3-2: Strategien der Hersteller von Drucksystemen im Consumerbereich, nach [Ger-09]

Brother	Konstruktive Besonderheiten der Tintenpatronen sind per Gebrauchsmuster geschützt
Canon	Tintenpatronen mit Mikrochips dienen zur Füllstandskontrolle und tragen eine starke Verschlüsselung
	Kombipatronen (Patronen mit Druckkopf) sind per Patent geschützt
Epson	Patronen mit Mikrochips dienen zur Füllstandskontrolle, tragen jedoch keine Verschlüsselung
Hewlett-Packard	Kombipatronen (Patronen mit Druckkopf) sind per Patent geschützt
Lexmark	Kombipatronen (Patronen mit Druckkopf) sind per Patent geschützt

3.3.1.1 Brother

Der Druckerhersteller Brother setzt Tintenpatronen ein, die konstruktiv herausfordernd sind. Die Füllstandsanzeige in den Tintentanks übernimmt ein mechanischer Schwimmer aus Plastik. Zusammen mit einer Lichtschranke wird so das Drucken ohne Tinte wirkungsvoll verhindert. Zudem sind der Tintenauslass und die Belüftung „so konstruiert, dass sie nur im Drucker geöffnet werden“ [Ger-09]. Diese Patronen sind als Gebrauchsmuster geschützt, Verletzungen dieses Gebrauchsmusters durch Wettbewerber werden verfolgt. [Ger-09]

3.3.1.2 Canon

Die Kombipatronen von Canon, bei denen Tintenpatronen und Druckkopf eine konstruktive Einheit bilden, sind per Patent vor Nachbau geschützt [Ger-09].

Bei einfachen Tintenpatronen arbeitet Canon seit 2005 mit Mikrochips, um den Füllstand zu überwachen und diesen dem Drucker mitzuteilen (siehe Abbildung 3-9). Diese Mikrochips sind zusätzlich durch eine starke Verschlüsselung geschützt, welche es dem Wettbewerb erschwert, kompatible Nachfüllpatronen zu entwickeln. Erst

nach etwa drei Jahren konnte die Verschlüsselung legal geknackt und es konnten alternative Tintenpatronen angeboten werden. [Ger-09]

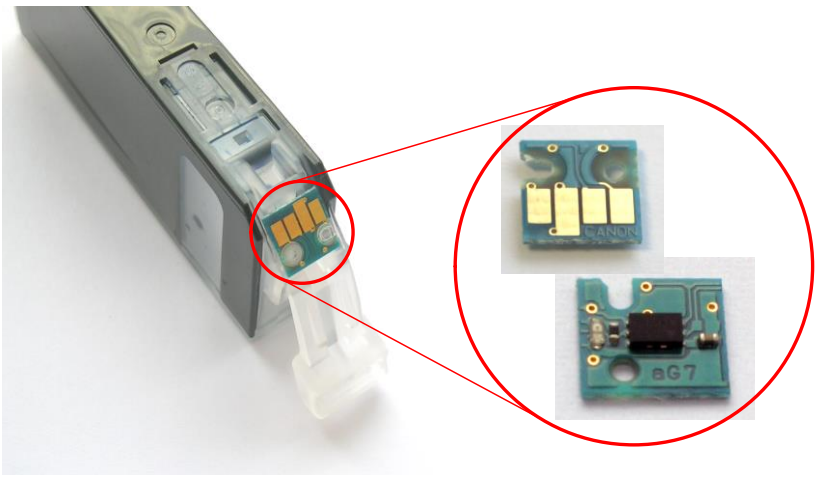


Abbildung 3-9: Einfache Tintenpatrone von Canon mit Mikrochip – Vorder- und Rückseite in vergrößerter Ansicht

Damit gibt es Alternativen zur Original-Tintenpatrone, welche von Wettbewerbern angeboten werden [Ger-09]:

- Komplettnachbau einer kompatiblen Tintenpatrone mit Mikrochip
- Nachfüllen vorhandener Original-Tintenpatronen und Rücksetzen der Mikrochips mit Hilfe eines sogenannten Chip-Resetters
- Nachfüllen vorhandener Original-Tintenpatronen ohne Rücksetzen der Mikrochips, das Drucksystem kann dann den Füllstand nicht mehr anzeigen
- Nachbau einer Tintenpatrone ohne Mikrochip, das Drucksystem kann dann den Füllstand nicht anzeigen
- Nachbau einer Tintenpatrone, manuelles Übertragen des Mikrochips von einer Original-Patrone auf den Nachbau und Rücksetzen der Mikrochips mit Hilfe eines sogenannten Chip-Resetters

3.3.1.3 Epson

Die Drucksysteme von Epson berechnen den verbleibenden Füllstand der Tintenpatronen rein auf Basis der Verbrauchsmengen bei Druck bzw. Düsenreinigung. Dieser Verbrauch wird für jede Patrone lokal auf einem angebrachten Mikrochip gespeichert. Da Epson auf eine Verschlüsselungstechnik verzichtet, sind kompatible Patronen relativ leicht zu entwickeln und das Angebot ist entsprechend breit. [Ger-09]

3.3.1.4 Hewlett-Packard

Hewlett-Packard verwendet stets Kombipatronen, bei denen ein Druckkopf integriert ist und die durch ein Patent vor Nachbau geschützt sind. Den Wettbewerbern bleibt so nur, Originalpatronen mit eigener Tinte wieder zu befüllen und am Markt anzubieten. [Ger-09]

3.3.1.5 Lexmark

Auch Lexmark verwendet in seinen Drucksystemen ausschließlich Tintenpatronen mit integriertem Druckkopf. Diese sind patentrechtlich geschützt, so dass den Wettbewerbern nur die Möglichkeit bleibt, Originalpatronen mit eigener Tinte wieder zu befüllen und zu verkaufen. Diesen Weg schränkt Lexmark zusätzlich dadurch ein, dass Kunden verpflichtet werden, leere Kartuschen zurückzugeben. Kartuschen ohne Rückgabepflicht sind von Lexmark nur gegen Aufpreis erhältlich. [Ger-09]

3.3.2 Überprüfung der Originalität von Dokumenten

Nachdem die Hersteller von Drucksystemen offenbar keine Funktion zur Authentifizierung einsetzen, werden in diesem Abschnitt Systeme untersucht, bei denen eine Authentifizierung – also die Prüfung deren Echtheit – eine zentrale Rolle spielt.

3.3.2.1 Überprüfung der Echtheit von Banknoten

Bei Banknoten gibt es verschiedene Sicherheitsmerkmale, die auf einem Geldschein integriert vorhanden sein können. Diese werden von der ausgebenden Zentralbank genau definiert und der Öffentlichkeit zugänglich gemacht, so dass jeder Wirtschaftsbeteiligte die Originalität von Banknoten überprüfen kann. Bei der Europäischen Gemeinschaftswährung sind die verwendeten Sicherheitsmerkmale einzusehen auf der Internetseite der Europäischen Zentralbank (EZB) oder der Deutschen Bundesbank [Deu-13a, EZB-13b].

Zur sicheren Prüfung der Originalität werden im Handel vielfach Banknotenprüfgeräte eingesetzt. Abbildung 3-10 zeigt die Prüfung fluoreszierender Sicherheitsmerkmale in einer 50-Euro-Banknote. Bei der einfachen Prüfung von Banknoten handelt es sich um die Authentifizierung anhand von Originalitätskennzeichen, beispielsweise fühlbares Relief durch Stichtiefdruck, Durchsichtsregister, Hologramme, Wasserzeichen, Mikrotexte, ultraviolette Farben, Kippfarben, Laserperforationen oder Sicher-

heitsfaden (siehe Anhang A.4.1.3.1, A.5.1.2, A.5.1.3, A.5.1.7, A.5.2.4, A.5.4.3.4, A.5.4.5, A.5.5.4.1, A.5.5.7).

Abbildung 3-10: Banknoten-Prüfgerät [Eco-13]

3.3.2.2 Authentifizierung mittels Ausweisdokument

Die Bundesdruckerei hat ein System entwickelt, mit dem es möglich ist, die Identität von Personen zu verifizieren. Dieses System ist modular aufgebaut und kann für die Anforderungen des Kunden angepasst werden. Ein Kunde kann beispielsweise ein Unternehmen oder ein Staat sein [Bun-05, Bun-12a]. Im Erkennungsprozess stützt sich die prüfende Instanz auf die Vertrauenswürdigkeit des Identifikationspapiers [Beh-01].

Für die Bundesrepublik Deutschland stellt die Bundesdruckerei den neuen deutschen Personalausweis her. Darauf sind unter anderem Familienname, Vornamen, Anschrift, Staatsangehörigkeit, Geburtsort und Geburtstag des Ausweisinhabers lesbar vermerkt [§ 5 PAuswG in Bun-09]. Als biometrische Daten sind ein Lichtbild, die Augenfarbe, und die Unterschrift abgedruckt [Beh-01 S. 13, BMI-13, BSI-13a, § 5 PAuswG in Bun-09]. Sämtliche, auf dem Personalausweis abgedruckten Daten sowie das biometrische Passbild und auf Wunsch zwei Fingerabdrücke werden zusätzlich auf einem integrierten, kontaktlos lesbaren Sicherheits-Chip gespeichert [§ 5 PAuswG in Bun-09, Bun-13b]. Die Identitätsprüfung einer Person anhand eines Ausweises und damit die Authentifizierung kann dann in drei Stufen erfolgen [Bun-05 S. 65 ff]:

1. Prüfung ohne Hilfsmittel:
   Überprüfung offener visueller und taktiler Sicherheitsmerkmale des Ausweises durch geschulte Mitarbeiter

2. Prüfung mittels zertifiziertem Lesegerät:
   Auslesen der auf dem Chip gespeicherten Daten und manueller Abgleich mit den abgedruckten Daten
3. Prüfung mittels zertifiziertem Lesegerät und Erfassungsgerät für biometrische Merkmale:
   Erfassen der notwendigen biometrischen Daten der Person und Abgleich mit den auf dem Chip gespeicherten biometrischen Daten

3.3.2.3 Überprüfung der Echtheit einer Fahrkarte

Bei der Authentifizierung einer Fahrkarte gibt es mehrere Verfahren. Einfache Fahrkarten können beispielsweise mittels Hologrammen und Tagesleuchtfarben (siehe Anhang A.5.1.3, A.5.4.3.3) gegen Kopieren geschützt werden. Neben der Gültigkeit für den jeweiligen Streckenabschnitt und Zeitpunkt werden diese Elemente visuell auf Originalität geprüft (siehe Abbildung 3-11).

Abbildung 3-11: Tagesleuchtfarben auf Fahrscheinen [Dia-13]

Bei personalisierten Fahrkarten (z. B. BahnCard 100, siehe Abbildung 3-12) wird neben der Gültigkeit und Originalität der Fahrkarte zusätzlich visuell geprüft, ob die besitzende Person auch Eigentümer der Fahrkarte ist, indem beispielsweise ein aufgedrucktes Foto mit der sich ausweisenden Person verglichen wird.

Abbildung 3-12: BahnCard 100 [Rhe-13]

Das Online-Ticket der Deutschen Bahn AG wiederum (siehe Abbildung 3-13) wird bei der Buchung durch einen Kunden mit einem persönlichen Dokument des Reisenden verknüpft: BahnCard, BonusCard Business, bahn.bonus Card, Kreditkarte, EC-Karte oder Personalausweis. Die Daten der Fahrkarte und des persönlichen Dokuments sowie der Name des Reisenden werden in einer Datenbank der Deutschen Bahn abgelegt (siehe Abbildung 3-14). Zusätzlich werden diese Daten verschlüsselt und in den auf der Fahrkarte abgedruckten Barcodes gespeichert. Der Kunde erhält das Ticket in Form einer PDF-Datei und kann sich dieses ausdrucken. [Dei-13, Thu-13, DB-12 S. 97 ff.]

Zur Authentifizierung erfasst das Zugbegleitpersonal mit seinem mobilen Terminal mittels Scan den 2D-Barcode. Dieser 2D-Barcode wird im mobilen Terminal entschlüsselt und damit die Echtheit und zeitliche Gültigkeit der Fahrkarte überprüft. Das mobile Terminal zeigt daraufhin die Fahrkartendaten an. Auch wird das persönliche Dokument des Reisenden eingelesen oder im Falle des Personalausweises manuell erfasst. Dies dient dazu, Missbrauch durch Vervielfältigung der Tickets zu verhindern. Der gesamte Kontrollprozess erfolgt offline. Um Mehrfachnutzungen von Online-Tickets auszuschließen werden die im mobilen Terminal gespeicherten Kontrolldatensätze zyklisch mit den Daten in der Datenbank verglichen. So können Fahrten mit bereits genutzten oder stornierten Fahrkarten ermittelt und verfolgt werden. [Dei-13, Thu-13, DB-12 S. 97 ff.]

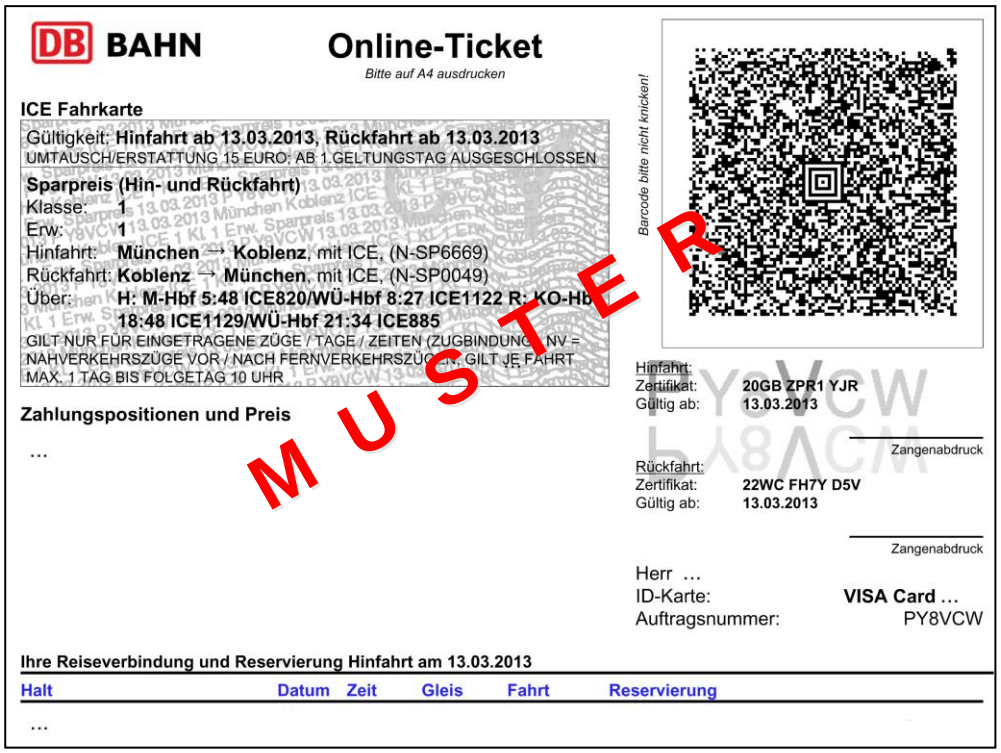


Abbildung 3-13: Online-Ticket der Deutschen Bahn AG

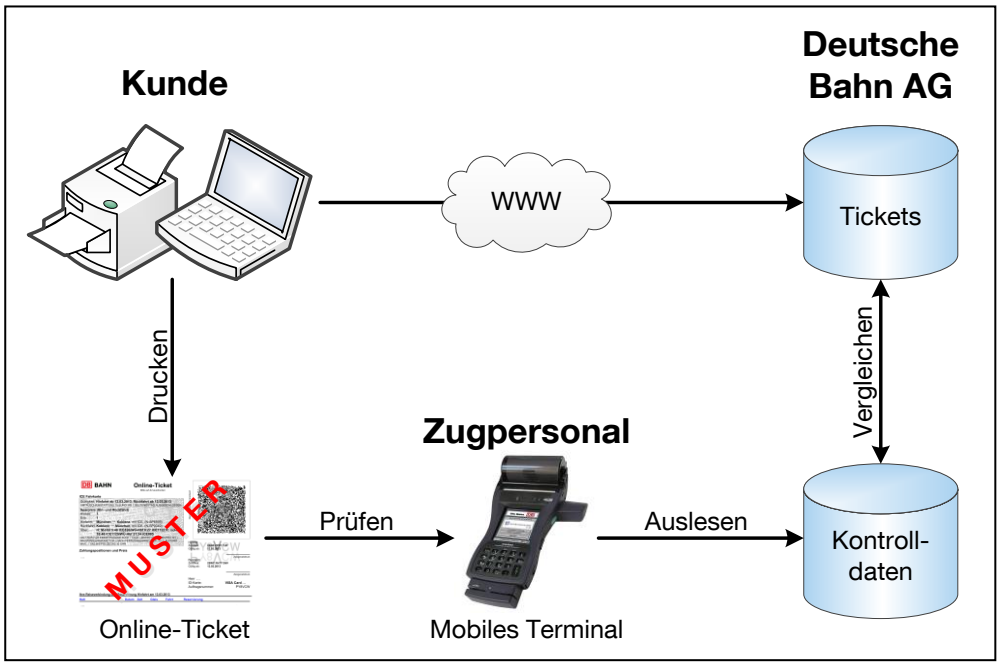


Abbildung 3-14: Kontrollprozess für Online-Tickets der Deutschen Bahn AG [Dei-13]

3.3.2.4 Electronic Cash System

Beim Electronic Cash System (EC-System) kann ein Kunde mit Hilfe seiner EC-Karte auf elektronischem Weg sein Girokonto belasten und bei einem Leistungsverkäufer einen offenen Betrag begleichen. Dafür führt der Kunde seine EC-Karte in ein elek-

tronisches Multifunktionsterminal ein. Mit der Eingabe seiner vierstelligen persönlichen Identifikationsnummer (PIN) bestätigt er seine Berechtigung zur Nutzung. In dem nachfolgenden Online-Datenaustausch erfolgt:

- Weitergabe der Kartendaten
- Prüfung der PIN
- Prüfung, ob die Karte gesperrt ist
- Feststellung des Verfügungslimits
- Feststellung des Kontoguthabens

Verläuft der Prüfprozess positiv und liegt der Betrag innerhalb des verfügbaren Finanzrahmens, wird der angeforderte Betrag beglichen und der Rechnungsbetrag vom Kundenkonto auf das Verkäuferkonto gebucht (siehe Abbildung 3-15). [Ban-05 S. 8, Bra-99 S. 231, Kor-09 S. 12]

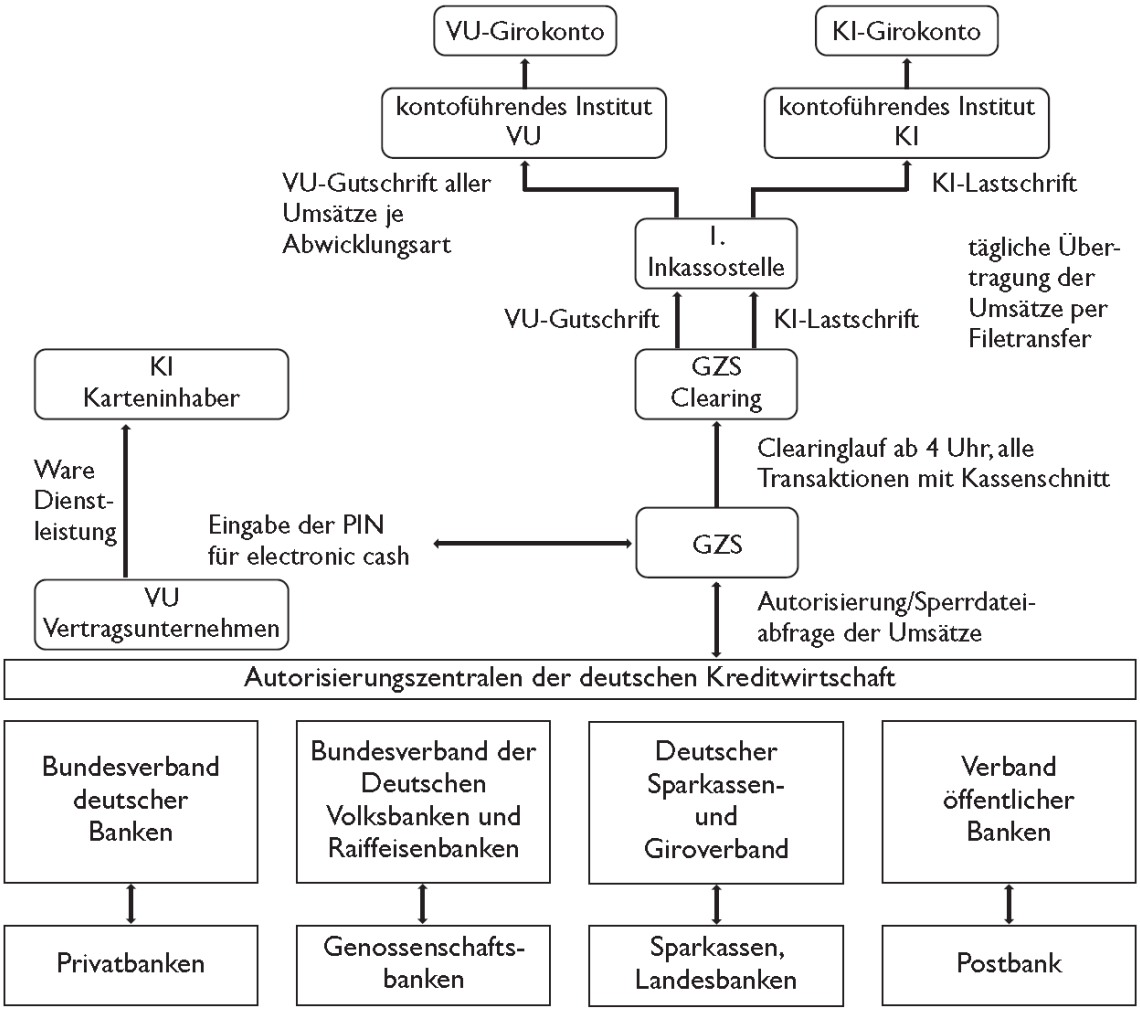


Abbildung 3-15: Ablauf einer EC-Transaktion der Gesellschaft für Zahlungssysteme (GZS) [Ban-05]

3.3.2.5 Zusammenfassung der Möglichkeiten und Systeme zur Überprüfung der Originalität von Dokumenten

Über die vier Beispiele

- Überprüfung der Echtheit von Banknoten, Abschnitt 3.3.2.1
- Authentifizierung mittels Ausweisdokument, Abschnitt 3.3.2.2
- Überprüfung der Echtheit einer Fahrkarte, Abschnitt 3.3.2.3
- Electronic Cash System, Abschnitt 3.3.2.4

hinweg ist feststellbar, dass der Einsatz technischer Hilfsmittel zur Authentifizierung und die datentechnische Vernetzung von Beispiel zu Beispiel zunehmen. Bei Banknoten kommen einfache Prüfgeräte zum Einsatz. Bei Ausweisdokumenten kann die Prüfung auch mit Hilfe von Geräten zum Abgleich von biometrischen Merkmalen des Ausweisinhabers mit den im Ausweis gespeicherten Daten erfolgen. Bei der Prüfung der Echtheit eines Online-Tickets erfolgt neben der Prüfung der Gültigkeit für die ausweisende Person auch ein Datenbankabgleich in einem verteilten, vernetzten IT-System – solche IT-Systeme sind auch im Bereich von T&T anzutreffen. Im EC-System ist ein Maximum an Sicherheit angelegt, um Zahlungsverkehre störungsfrei und korrekt elektronisch im global verteilten, vernetzten IT-System ablaufen zu lassen.

Diese Systeme arbeiten alle mit einer Form der Authentifizierung. Teilweise auf Basis von Sicherheitsmerkmalen, teilweise mit Verschlüsselungsalgorithmen, teilweise mit sofortigen oder zeitlich nachgelagerten Datenbankabgleichen. Jedoch arbeitet keines dieser Systeme mit Sicherheitsmerkmalen als integraler Bestandteil eines technischen Systems zur Authentifizierung eines Objektes.

Dies hat seine Gründe. Bei Banknoten wäre eine permanente, eventuell sogar weltweite Überprüfung der Sicherheitsmerkmale in Verknüpfung mit einem Tracking nicht praktikabel. Bei Ausweisdokumenten ist ein Tracking aus Datenschutzgründen untersagt. Bei Fahrkarten ist es technisch nicht umsetzbar, dass beim Ausdruck eines Online-Tickets durch einen Kunden ein oder mehrere Sicherheitsmerkmale verwendet werden. Beim EC-System verlässt man sich auf die datenseitige Sicherheit und kryptografische Algorithmen. Dennoch geben diese Beispiele einen tiefen Einblick, wie entsprechende technische Systeme gestaltet sein können, um daraus für das zu entwickelnde Produktpiraterie-Schutzsystem zu lernen.

Mit diesen Erkenntnissen können die entsprechenden Einträge in der zusammenfassenden Übersicht in Tabelle 3-3 in den Zeilen zu „3.3.2 Überprüfung der Originalität von Dokumenten“ vorgenommen werden.

3.3.3 Schutz des Arzneimittelvertriebs vor gefälschten Arzneimitteln

Als letztes System zur Absicherung der Originalität von Objekten wird ein System im Pharmavertrieb untersucht. Auch im Bereich von Arzneimitteln gibt es weltweit ein wachsendes Risiko durch Fälschungen [BMG-13, Sec-13]. Als Reaktion darauf wurde die EU-Richtlinie 2011/62/EU „zur Änderung der Richtlinie 2001/83/EG zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel hinsichtlich der Verhinderung des Eindringens von gefälschten Arzneimitteln in die legale Lieferkette“ verabschiedet. In Artikel 54 wird darin folgendes vorgegeben:

„Die äußere Umhüllung oder […] die Primärverpackung jedes Arzneimittels muss die nachstehenden Angaben aufweisen:
[…]
Sicherheitsmerkmale, die es Großhändlern und Personen, die zur Abgabe von Arzneimitteln an die Öffentlichkeit ermächtigt oder befugt sind, ermöglichen,

- die Echtheit des Arzneimittels zu überprüfen; und
- einzelne Packungen zu identifizieren;

sowie eine Vorrichtung, die es ermöglicht, zu überprüfen, ob die äußere Umhüllung manipuliert worden ist.“ [Amt-01, Amt-11]

Diese EU-Richtlinie wurde in Deutschland mit dem zweiten Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften im Jahr 2012 in nationales Recht überführt [Bun-12b]. Eine Frist zur Realisierung dieser gesetzlichen Vorgabe existiert noch nicht, Angaben von Experten zufolge wird voraussichtlich eine im Jahr 2017 ablaufende Frist zur Realisierung eingerichtet [Tho-13].

Wie der EU-Richtlinie 2011/62/EU bzw. dem entsprechenden nationalen deutschen Gesetz entnommen werden kann, ist nicht spezifiziert, welche Sicherheitsmerkmale zum Einsatz kommen sollen bzw. wie deren Prüfung erfolgen soll.

Die Initiative securPharm e.V. zum Schutz des deutschen Arzneimittelvertriebs vor dem Eindringen gefälschter Arzneimittel arbeitet daher in einem Pilotprojekt daran, die Supply-Chain von Arzneimitteln abzusichern (siehe Abbildung 3-16): „Bei der Produktion wird jede einzelne Packung mit einer individuellen Seriennummer verse-

hen. Diese Seriennummer wird zusammen mit der PZN [Pharmazentralnummer, Anm. d. Verf.], Charge und Verfalldatum als Data Matrix Code auf die Packung aufgedruckt. Im Anschluss werden diese Angaben in einer Datenbank der pharmazeutischen Unternehmen gespeichert. Zur Verifikation einer Packung scannt das Apothekenpersonal den neuen Data Matrix Code von der Packung. Im Hintergrund findet die Überprüfung von Seriennummer und Produktnummer gegenüber der Datenbank statt. Das erfolgt unter Zwischenschaltung eines zweiten Systems (Apotheken-System), so dass zu keinem Zeitpunkt ein Hersteller bzw. pharmazeutischer Unternehmer nachvollziehen kann, welche Apotheke welches Arzneimittel abgegeben hat.“ [Sec-13]

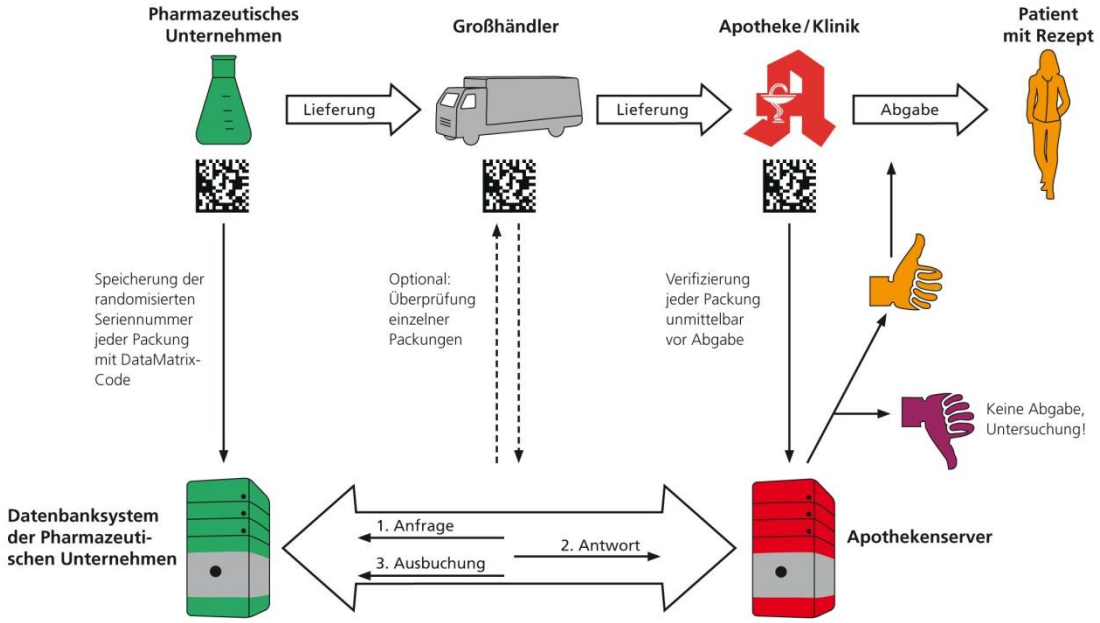


Abbildung 3-16: End-to-End-Kontrollsystem für den securPharm-Piloten [Sec-13]

Damit ist klar, dass auch dieses System nicht mit Sicherheitsmerkmalen, sondern mit einfachen 2D-Barcodes arbeitet und die Authentifizierung mittels eines Online-Datenbankabgleichs stattfindet. Da die 2D-Barcodes einfach kopierbar sind, liegt die Sicherheit in der 20-stelligen Seriennummer, die für jede Arzneimittelpackung als Zufallszahl erzeugt wird und neben den Ziffern 0-9 auch die Buchstaben A-Z erlaubt [Sec-12 S. 6, S. 15]. Zudem ist eine Seriennummer nur im Zeitraum zwischen Herstellung und Verkauf gültig und damit für einen Fälscher nahezu nicht zu erraten. Dennoch hat der 2D-Barcode keine präventive Wirkung wie ein unkopierbares Sicherheitsmerkmal. Insbesondere realisiert auch dieses System kein T&T. Damit können in der zusammenfassenden Übersicht in Tabelle 3-3, Zeile „3.3.3 Schutz des

Arzneimittelvertriebs vor gefälschten Arzneimitteln“ entsprechende Einträge vorgenommen werden.

3.4 Zusammenfassung und Darstellung des Forschungsbedarfs

Wie in den Abschnitten 3.1 bis 3.3 deutlich wird, gibt es im Stand der Technik aktuell zwei große Bereiche. Einerseits die am Markt verfügbaren Sicherheitsmerkmale, welche Originalwaren fälschungssicher kennzeichnen und authentifzierbar machen. Andererseits gibt es technische Systeme, die entweder ein T&T ermöglichen oder eine Authentifizierung – allerdings nicht auf Basis von Sicherheitsmerkmalen.

Es gibt lediglich zwei Ansätze, die sowohl das T&T für Güter als auch deren Authentifizierung anbieten: „Tracking&Tracing in der Luft- und Raumfahrtbranche“ und „Software zur Authentifizierung von Produkten und Dokumenten“. Allerdings arbeiten auch diese beiden Systeme bei der Authentifizierung nicht auf Basis von Sicherheitsmerkmalen, sondern auf Basis von einmaligen Nummern und Codes bzw. 2D-Barcodes und Datenbankabgleichen. Diese Erkenntnisse aus den vorangegangenen Abschnitten sind in Tabelle 3-3 als Übersicht zusammengefasst.

Im Falle der Luft- und Raumfahrtbranche (siehe Abschnitt 3.2.3) können diese Nummern und Codes somit auf nachgebaute Bauteile kopiert werden. Systemseitig wird dies zwar vor dem Verbau des jeweiligen Bauteils festgestellt, aber der präventive Charakter, den die Verwendung von Sicherheitsmerkmalen mit sich bringt, ist damit nicht vorhanden. Zudem ist bei zwei äußerlich gleichen Bauteilen mit denselben Nummern und Codes nicht klar, welches der beiden Bauteile das Original ist.

Ähnlich verhält es sich bei der Software zur Authentifizierung von Produkten und Dokumenten, das mit 2D-Barcodes arbeitet (siehe Abschnitt 3.2.4). Auch 2D-Barcodes können auf kopierte Produkte übertragen werden. Bei der untersuchten Lösung können jedoch zusätzlich Sicherheitsmerkmale auf den Originalwaren für deren Authentifizierung herangezogen werden. Aber da der Authentifizierungsschritt nicht Teil des technischen Systems ist, kann das Prüfergebnis nicht dokumentiert werden, um Auseinandersetzungen auf Basis dieser objektiven Daten schnell klären zu können.

Das Ziel der vorliegenden Arbeit ist es, ein technisches Produktpiraterie-Schutzsystem für den Maschinen- und Anlagenbau zu entwickeln, das eine Authentifizierung auf Basis von Sicherheitsmerkmalen als systemischer Teil eines technischen Gesamtsystems ermöglicht. Die Prüfergebnisse sollen dabei erfasst und dokumentiert werden. Ein System, welches dies vereinigt, wirkt zusätzlich präventiv und schreckt bereits vor dem Kopieren von Bauteilen ab (siehe Ziele in Abschnitt 1.2.2, S. 8). Da ein solches System nicht existiert, besteht in diesem Bereich umfassender Forschungsbedarf.

Tabelle 3-3: Eigenschaften von Sicherheitsmerkmalen sowie existierender Systeme zur Nachverfolgung

Abschnittsnummer und Überschrift	Authentifizierung	Verwendung von Sicherheitsmerkmalen	Tracking & Tracing	Integration mehrerer Technologien zur Authentifizierung in einem technischen Schutzsystem
3.1 Sicherheitsmerkmale	ja	ja	nein	nein [1]
3.2 Existierende Systeme zur Nachverfolgung und zur Sicherstellung der Originalität	-			
3.2.1 Tracking&Tracing-Systeme allgmein	nein	nein	ja	nein
3.2.2 Tracking&Tracing bei KEP-Diensten	nein	nein	ja	nein
3.2.3 Tracking&Tracing in der Luft- und Raumfahrtbranche	ja [2]	nein	ja	nein
3.2.4 Software zur Authentifizierung von Produkten und Dokumenten	ja [3]	(ja) [3]	ja	nein [3]
3.3 Existierende Systeme zur Sicherstellung der Originalität	-			
3.3.1 Originalität einer Tintenpatrone	-			
3.3.1.1 Brother	nein	nein	nein	nein
3.3.1.2 Canon	nein	nein	nein	nein
3.3.1.3 Epson	nein	nein	nein	nein
3.3.1.4 Hewlett-Packard	nein	nein	nein	nein
3.3.1.5 Lexmark	nein	nein	nein	nein
3.3.2 Überprüfung der Originalität von Dokumenten	-			
3.3.2.1 Überprüfung der Echtheit von Banknoten	ja	ja	nein	nein
3.3.2.2 Authentifizierung mittels Ausweisdokument	ja	ja	nein	nein
3.3.2.3 Überprüfung der Echtheit einer Fahrkarte (Online-Ticket)	ja	nein	nein	nein
3.3.2.4 Electronic Cash System	ja	nein	nein	nein
3.3.3 Schutz des Arzneimittelvertriebs vor gefälschten Arzneimitteln	ja [2]	nein	nein	nein
Ziel Technisches Produktpiraterie-Schutzsystem für Maschinen- & Anlagenbau	**ja**	**ja**	**ja**	**ja**

[1] Zwar sind verschiedene Sicherheitsmerkmale in ein Produkt integrierbar, diese stehen aber nebeneinander zur Authentifizierung zur Verfügung und sind insbesondere nicht Bestandteil eines integrierten technischen Schutzsystems.

[2] Authentifizierung durch Abgleich einer Nummer oder eines Codes über eine Online-Datenbankabfrage, nicht auf Basis von Sicherheitsmerkmalen.

[3] Authentifizierung durch Online-Abgleich eines 2D-Barcodes mit Hilfe einer Datenbankabfrage, nicht auf Basis von Sicherheitsmerkmalen. Die neben dem 2D-Barcode angebrachten Sicherheitsmerkmale muss der Nutzer eigenständig authentifizieren. Dieser Schritt findet somit nebenläufig statt und ist nicht Teil des technischen Schutzsystems. Das Prüfergebnis liegt nur kurzzeitig dem jeweiligen Nutzer vor, eine systemseitige Erfassung und Dokumentation des Prüfergebnisses erfolgt nicht.

4 Aktueller Stand der Wissenschaft und Forschung

In Kapitel 3 wurde aufgezeigt, dass es aktuell kein technisches System gibt, das die in Abschnitt 1.2.2, S. 8 formulierten Ziele und Funktionen aufweist. In diesem Kapitel wird untersucht, ob es neue, passende Lösungen im Bereich der Wissenschaft und Forschung gibt.

4.1 Überblick über den aktuellen Stand der Wissenschaft und Forschung

Da sich Produkt- und Markenpiraterie zum „Verbrechen des 21. Jahrhunderts“ entwickelt hat [Den-08] und bereits im Sommer 2005 von der Internationalen Handelskammer (ICC: International Chamber of Commerce) als „außer Kontrolle“ bezeichnet wurden [Cat-05], ist es nicht verwunderlich, dass es national wie international zahlreiche Veröffentlichungen in Buchform, Zeitschriften, Zeitungen und Online-Portalen gibt. Die Internet-Suchmaschine Google lieferte am 29. Januar 2013 bei der Suche nach „Produktpiraterie“ 395.000, bei der Suche nach „Counterfeiting“ (engl.: Produktpiraterie) sogar 6.920.000 Ergebnisse [Goo-13a, Goo-13b].

Im Zeitraum 2007 bis 2011 wurden durch das Bundesministerium für Bildung und Forschung (BMBF) innerhalb des Rahmenkonzepts „Forschung für die Produktion von morgen“, 21. Bekanntmachung „Innovationen gegen Produktpiraterie“ elf Forschungsprojekte gefördert, in denen und deren Umfeld weitere wertige Ergebnisse im Themenbereich gewonnen und veröffentlicht werden konnten. [BMBF-06, KIT-12b, Hei-12]

Existierende Arbeiten zur Fragestellung, wie man Produktpiraterie begegnen könne, lassen sich danach einteilen, ob diese technische Sicherheitsmerkmale (siehe Definition in Abschnitt 2.7, S. 27) oder Maßnahmen im Bereich der Produktentwicklung, Produktion, IT-Sicherheit, Betriebswirtschaft, Recht oder Politik beschreiben. Zudem, ob in diesen Quellen Bewertungs-, oder Auswahlmethoden angegeben sind

und ob eine Integration von Sicherheitsmerkmalen und -technologien zur Einbindung in technische Gesamtsysteme aufgezeigt wird.[15]

Tabelle 4-1 gibt einen Einblick in die aktuelle Wissenslandschaft. Das Gros der Quellen beschränkt sich dabei darauf, Technologien für Sicherheitsmerkmale und Maßnahmen gegen Produktpiraterie zu benennen und zu beschreiben (siehe Punkte 1 bis 4). Dann gibt es Quellen, welche zusätzlich eine Auswahlmethode für Maßnahmen und / oder Technologien darstellen (Punkte 5 bis 7). Lediglich ein kleiner Teil der verfügbaren Veröffentlichungen beschäftigt sich mit der Integration von Technologien für Sicherheitsmerkmale in ein technisches Gesamtsystem zur Authentifizierung von Objekten (Punkt 8). Die wenigsten Arbeiten vermitteln eine ganzheitliche Sicht zur Beschreibung von Technologien für Sicherheitsmerkmale mit der Darstellung einer Auswahlmethode und deren Einbindung in technische Gesamtsysteme zur Authentifizierung von Objekten (Punkt 9).

[15] Der Begriff Maßnahmen ist hier komplementär zum Begriff Sicherheitsmerkmal belegt und soll alle Möglichkeiten außerhalb von Sicherheitsmerkmalen zum Schutz gegen Produktpiraterie umfassen. Dieser Begriff wurde bereits eingeführt und es gibt eine Übersicht existierender Maßnahmen in Abschnitt 2.4, S. 22.

Tabelle 4-1: Kategorisierung und Einordnung ausgewählter Quellen

1) Beschreibung von einzelnen Technologien für Sicherheitsmerkmale: Alp-13, Aus-13b, Beh-07, Beh-13a, Boc-13, Dat-13a, Dat-13b, Dat-13c, Fra-11, Hot-11, Hup-08, Hot-11, Ins-13, Lou-13, Pfa-07, Pol-13
2) Beschreibung von Technologien für Sicherheitsmerkmale als Überblick: Aus-13a, Cor-13, Kok-02, Krä-06, Mal-05, Pri-13, Rat-13, Sil-08, Völ-13
3) Beschreibung möglicher Maßnahmen als Überblick: Wur-11
4) Beschreibung von Technologien für Sicherheitsmerkmale und Maßnahmen als Überblick: Hop-03, Kro-06, Sit-06, Wil-07, Win-07
5) Beschreibung von Technologien für Sicherheitsmerkmale mit Darstellung einer Auswahlmethode: Pro-12
6) Beschreibung von Maßnahmen mit Darstellung einer Bewertungs- und / oder Auswahlmethode: Abe-10 [1], Gün-11b [2], Nee-07, Sch-10a
7) Beschreibung von Technologien für Sicherheitsmerkmale und Maßnahmen mit Darstellung einer Bewertungs- und / oder Auswahlmethode: Abe-10 [3], Abe-11, Fuc-06, Gau-12, ICC-06, Kle-10 [4], Mei-11, Ste-11a, Wel-07
8) Beschreibung einer Technologie für Sicherheitsmerkmale und deren Einbindung in technische Gesamtsysteme zur Authentifizierung von Objekten: Abr-10 [5], Abr-13 [6], Sta-07, Sta-08
9) Beschreibung von Technologien für Sicherheitsmerkmale mit Darstellung einer Auswahlmethode und der Einbindung verschiedener Technologien in technische Gesamtsysteme zur Authentifizierung von Objekten: Abe-10 [2], Gün-11a [2], Gün-11c [2], Gün-11d [2], Sto-12 [2]

[1] Ergebnisse Forschungsprojekte KoPira (S. 25-63) und ProOriginal (S. 64-95)

[2] Ergebnisse Forschungsprojekt ProAuthent unter Mitarbeit des Autors der vorliegenden Arbeit [in Abe-10 die S. 96-151]

[3] Ergebnisse Forschungsprojekt KoPiKomp (S. 152-207)

[4] Ergebnisse Forschungsprojekte PiratPro (S. 74-130) und PROTACTIVE (S. 19-73)

[5] Ergebnisse Forschungsprojekte EZ-Pharm (S. 74-137), O-PUR (S. 26-73) und MobilAuthent (S. 138-182)

[6] Ergebnisse Forschungsprojekt MobilAuthent

4.2 Abgrenzung zum aktuellen Stand der Wissenschaft und Forschung

Die vorliegende Arbeit ist in Tabelle 4-1 unter Punkt 9 einzuordnen, denn das Ziel der vorliegenden Arbeit ist ein technisches System, das mit Kennzeichnung und Authentifizierung arbeitet und eine dauerhafte Unterscheidbarkeit zwischen Original und Kopie ermöglicht. Dabei soll eine ganzheitliche Sicht erarbeitet werden: von der Bestimmung schützenswerter Bauteile über die Auswahl passender Kennzeichnungs- und Authentifizierungstechnologien bis hin zur Integration dieser Technologien in ein technisches Gesamtsystem zur dokumentierten Authentifizierung von Objekten. Überdies soll das System mit funktionserweiternden Zusatznutzen ergänzt werden (siehe Abschnitt 1.2.2, S. 8).

Diese Inhalte sind gegenüber dem aktuellen Stand der Forschung neu, wie die nachfolgende Analyse zeigt. Für die Abgrenzung der vorliegenden Arbeit gegenüber dem aktuellen Stand der Forschung ist es ausreichend, die in Tabelle 4-1 unter Punkt 8 und 9 gelisteten Quellen genauer zu untersuchen.

Eine vergleichbar ganzheitliche Annäherung an das Thema der Kennzeichnung von Bauteilen für eine Authentifizierung auf technischem Weg ist in den Arbeiten in Tabelle 4-1 unter Punkt 9 gegeben. In den genannten Quellen sind ausschnittsweise Inhalte des Forschungsprojekts „ProAuthent – Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau“ [16] [fml-13a, fml-13b] veröffentlicht. In diesem Forschungsprojekt hat der Autor der vorliegenden Dissertation die Grundlagen erarbeitet und in den unter Punkt 9 genannten Quellen vorveröffentlicht. Diese Inhalte werden daher in der vorliegenden Arbeit aufgegriffen, erweitert und verallgemeinert.

Die in Tabelle 4-1 unter Punkt 8 genannten Quellen beschreiben Technologien für Sicherheitsmerkmale und verfolgen zusätzlich das Ziel, diese in technische Gesamtsysteme einzubinden. Dabei werden lediglich Einzeltechnologien betrachtet:

[16] Dieses Forschungs- und Entwicklungsprojekt wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmenkonzept „Forschung für die Produktion von morgen“ gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

- Forschungsprojekt EZ-Pharm (siehe Abschnitt 4.2.1):
  RFID-basierte Echtheitsprüfung für Medikamente auf der Ebene einzelner Verpackungen [Abr-10 S. 126 ff.]
- Forschungsprojekt O-PUR (siehe Abschnitt 4.2.2):
  2D-Codes als Sicherheitsmerkmal auf Produkten und Verpackungen [Abr-10 S. 26 ff.]
- Forschungsprojekt MobilAuthent (siehe Abschnitt 4.2.3):
  Einsatz von RFID-Transpondern mit kryptografischen Funktionen [Abr-10 S. 138 ff., Abr-13]
- Stufenmodell zur Authentifizierung von Objekten mittels RFID (siehe Abschnitt 4.2.4):
  Verwendung von RFID-Transpondern als Sicherheitsmerkmal für Objekte in einem Produktpiraterie-Schutzsystem mit verschiedenen Stufen [Sta-07, Sta-08]

4.2.1 EZ-Pharm

Im Forschungsprojekt „EZ-Pharm – Anwendung elektronischer Echtheitszertifikate an Verpackungen entlang der Pharmaversorgungskette“ wurde eine RFID-basierte Echtheitsprüfung für Medikamente auf der Ebene einzelner Verpackungen realisiert (Abr-10 S. 126, IPH-12). Dabei bildet eine elektronisch gesicherte Verpackung die Basis, bei der RFID-Antennen mit Silberleitfarbe direkt auf den Karton der Medikamentenfaltschachtel gedruckt und mit einem Chip bestückt werden (siehe Abbildung 4-1). So bildet der RFID-Transponder eine Einheit mit der Faltschachtel und ist vor einfacher manueller Übertragung auf eine Kopie geschützt [Abr-10 S. 98 ff.].

Zur Authentifizierung eines Medikaments erfolgt ein Datenbankabgleich mit der Seriennummer des Medikaments und den am Transponder vorhandenen dynamischen Daten [Abr-10 S. 126]. Diese werden an jedem Identifikationspunkt der Pharmaversorgungskette durch den Eintrag der jeweiligen Orts- und Zeitinformation auf dem Transponder wie auch der zentralen Datenbank fortgeschrieben [Abr-10 S. 96 f.].

Abbildung 4-1: Faltschachteln für Pharmaprodukte mit RFID-Transponder (links) und Testlesung einer bestückten Faltschachtel [IPH-12 und Abr-10 S. 113]

Neben der Weiterentwicklung der RFID-Technologie zum integralen Bestandteil einer Verpackung wurde in diesem Projekt ein dynamisches Datenmodell entwickelt. Ein einfaches Klonen, d. h. die Kopie der Daten auf einen funktionsgleichen Transponder zur Erzeugung einer Kopie, wird jedoch durch dieses System nicht verhindert, denn sämtliche Daten werden im Read-Write-Bereich des Transponders abgelegt und sind so offen zugänglich. Die Daten können daher leicht auf einen anderen Transponder kopiert werden, was systemseitig nicht zwingend erkannt wird. So könnte auch eine Kopie beim Datenbankabgleich als Original bestätigt werden. Zudem wird in diesem System allein RFID als Technologie eingesetzt, weitere Sicherheitstechnologien bleiben unberücksichtigt.

4.2.2 O-PUR

Im Forschungsprojekt „O-PUR – Originäres Produktsicherungs- und Rückverfolgungskonzept“ wurden Produkte und Verpackungen unter Ausnutzung der stochastischen Schwankungen im Markierprozess bei der Aufbringung eines 2D-Codes auf ein Substrat (z. B. Bedrucken von Papier oder Kunststoff, Prägen oder Gravieren von Metall) fälschungssicher gekennzeichnet [Ein-12, Gau-10 S. 20 f.]. Die Prüfung erfolgt in diesem System wahlweise in zwei Stufen: die autarke Prüfung mittels eines sogenannten NanoGrids bietet Schutz gegen Kopieren (siehe Abbildung 4-2), der Datenbankabgleich des einmaligen EpiCodes und / oder des je Charge einmaligen ClusterCodes bestätigt zweifelsfrei die Originalität [Abr-10 S. 32].

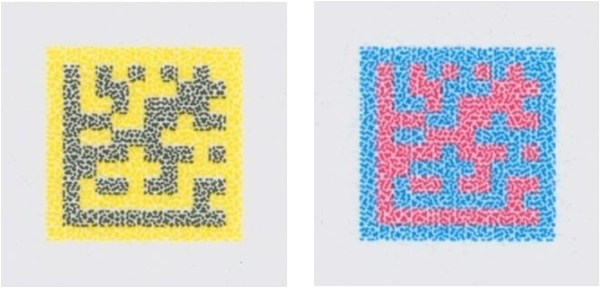


Abbildung 4-2: Überlagerung eines herkömmlichen 2D-Barcodes mit einem NanoGrid [Abr-10 S. 33]

Der Fokus des Projektes lag auf der Entwicklung und Verwendung einer einzelnen Technologie zum Schutz von Waren. Ein T&T der gekennzeichneten Objekte oder andere weiteren Funktionen, die das System realisieren könnte, bietet das System nicht.

4.2.3 MobilAuthent

Das Forschungsprojekt MobilAuthent entwickelte ein System zur branchenübergreifenden globalen mobilen Produktauthentifizierung mittels RFID [Abr-13]. Dabei kommen Transponder zum Einsatz, welche über kryptografische Funktionen verfügen. Neben der reinen Authentifizierung von Objekten mittels Datenaustausch zwischen Transponder und einer Datenbank (z. B. Challenge-Response-Verfahren) werden in diesem System auch Funktionalitäten des T&T bereitgestellt [Abr-10 S. 140 ff.]. Die Lösung des Projektes ist schematisch in Abbildung 4-3 zu sehen.

Das Projekt konzentriert sich auf RFID und setzt Transponder mit kryptografischen Funktionen ein. Andere Sicherheitsmerkmale lässt es außer Acht. Neben T&T gibt es die Möglichkeit, produktindividuelle Daten zur Beschreibung der Eigenschaften eines Produktes als Stammdaten zu hinterlegen. Darüber hinausgehende Funktionalitäten sind nicht integriert.

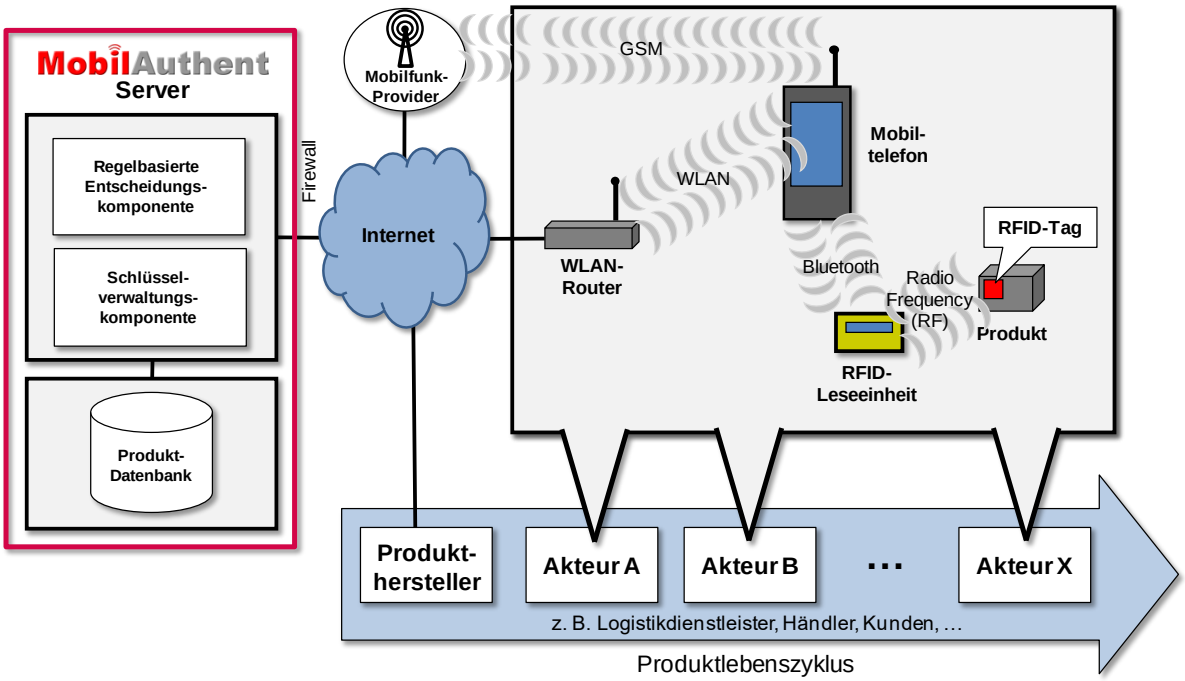


Abbildung 4-3: Komponenten der Lösung von MobilAuthent [Abr-10 S. 174]

4.2.4 Stufenmodell zur Authentifizierung von Objekten mittels RFID

Staake nutzt in seinem Entwurf eines Produktpiraterie-Schutzsystems allein RFID als Sicherheitsmerkmal für Objekte. Dabei werden verschiedene Stufen dargestellt, wobei zur Authentifizierung immer eine Datenbankverbindung notwendig ist. Diese reichen vom einfachen Datenbankabgleich von auf dem Transponder gespeicherten einmaligen Nummern über Plausibilitäts-Checks auf Bewegungsdaten der Objekte (nur aufzählend angeführt) bis hin zu Challenge-Response-Verfahren mittels kryptografischen Transpondern [Sta-07, Sta-08].

Neben RFID werden keine weiteren Sicherheitsmerkmale in das System einbezogen. Zudem gibt es keine Darstellung, wie über die reine Authentifikation von Objekten systemseitig weitere Funktionen realisiert und angeboten werden könnten.

4.3 Zusammenfassung

Analog zu Kapitel 3 lässt sich auch für den aktuellen Stand der Wissenschaft und Forschung eine Tabelle aufstellen (siehe Tabelle 4-2). Darin werden die im vorigen Abschnitt untersuchten Forschungsprojekte und -systeme mit ihren Eigenschaften und Funktionen gelistet. Dabei ist festzustellen, dass auch in der Forschung bisher kein System beschrieben ist, das verschiedene Sicherheitsmerkmale einsetzt, um

Produkte als Originale zu kennzeichnen, an Prüfpunkten zu authentifizieren und diese Prüfpunkte zu einem sicheren T&T-System zu kombinieren.

Tabelle 4-2: Eigenschaften der relevanten Systeme aus Wissenschaft und Forschung zur Authentifizierung von Objekten

Abschnittsnummer und Überschrift	Authentifizierung	Verwendung von Sicherheitsmerkmalen	Tracking & Tracing	Integration mehrerer Technologien zur Authentifizierung in einem technischen Schutzsystem
4.2.1 EZ-Pharm	ja [1]	nein	ja	nein
4.2.2 O-PUR	ja [2]	ja [2]	nein	nein
4.2.3 MobilAuthent	ja [3]	ja [3]	ja	nein
4.2.4 Stufenmodell zur Authentifizierung von Objekten mittels RFID	ja [4]	ja [4]	nein	nein
Ziel Technisches Produktpiraterie-Schutzsystem für den Maschinen- und Anlagenbau	**ja**	**ja**	**ja**	**ja**

[1] Einsatz von RFID-Transpondern zur Objektauthentifizierung mittels Datenbankabgleich
[2] Einsatz kopiersicherer 2D-Codes zur Objektauthentifizierung, mit und ohne Datenbankabgleich
[3] Einsatz von Krypto-Transpondern und Datenbankabgleich
[4] In der höchsten Ausbaustufe Einsatz von Krypto-Transpondern und Datenbankabgleich

Des Weiteren ist in den in Abschnitt 4.2 untersuchten Projekten kein Vorgehen angegeben, wie einerseits schützenswerte Bauteile und andererseits passende Kennzeichnungs- und Authentifizierungstechnologien bestimmt werden können. Auch gibt es kein System, welches über die Funktionalitäten des T&T weitere Systemfunktionalitäten für Hersteller und Kunden mit den gewählten Sicherheitsmerkmalen verknüpft, um das Gesamtsystem für beide Parteien attraktiv zu gestalten.

Ein System, welches dies vereinigt, wirkt durch die verwendeten Sicherheitsmerkmale präventiv, kann somit Bauteile bereits vor dem Kopieren schützen und ist darüber hinaus aufgrund der umfangreichen Systemfunktionen interessant für Hersteller und Kunden. In diesem Bereich besteht umfassender Forschungsbedarf.

5 Systemischer Ansatz

Das After-Sales-Geschäft mit Komponenten und Ersatzteilen ist ein wichtiges Standbein des Maschinen- und Anlagenbaus, da die Unternehmen in diesem Bereich wesentliche Anteile der Gewinne erwirtschaften (siehe Abschnitt 1.1.2, S. 8). Diesen wirtschaftlichen Erfolg machen sich redliche sowie unredliche Wettbewerber zu Nutze. Sie setzen genau an diesem Punkt an und kopieren Komponenten und Ersatzteile des Originalherstellers (siehe Abschnitt 1.1.4, S. 5) mit Schäden und Folgen für Originalhersteller, Verbraucher und das Gemeinwesen (siehe Abschnitt 2.3, S. 19).

Der Standardablauf von Entwicklung, Herstellung, Verkauf und Betrieb von Maschinen bzw. Anlagen bei einem Originalhersteller und seinem Vertriebssystem ist in Abbildung 5-1 dargestellt. Dabei ist auch der Vorgang der Nachbestellung von Komponenten oder Ersatzteilen beim Originalhersteller durch den Betreiber einer Maschine / Anlage abgebildet. Mit Komponenten kann der Betreiber seine Maschine / Anlage erweitern, Ersatzteile erhalten die Funktionsfähigkeit. Solange Originalkomponenten und -ersatzteile eingesetzt werden, kann von einem „problemlosen Betrieb“ gesprochen werden. Sobald auf einer Maschine / Anlage jedoch Kopien von Komponenten und Ersatzteilen wissentlich oder unwissentlich zum Einsatz kommen, kann dieser originäre problemlose Ablauf gestört werden. Und für den Kunden und Hersteller können daraus alle in Abschnitt 2.3, S. 19 dargestellten Schadensarten entstehen.

Um diesen problembehafteten Ablauf durch die Herstellung und den Vertrieb von Kopien zu verhindern oder wenigstens zu erschweren und Kopien erkennbar zu machen, kann für Komponenten und Ersatzteile ein System aus Kennzeichnung und Authentifizierung der Originalwaren zum Einsatz kommen. Damit soll für alle Wirtschaftsbeteiligten in der gesamten Wertschöpfungs- und Logistikkette über den gesamten Lebenszyklus des Bauteils eine nachweisbare Unterscheidbarkeit zwischen Originalware und Kopie gewährleistet werden. Um dies zu erreichen, werden in dieser Arbeit zwei existierende Ansätze zusammengeführt. Einerseits der Ansatz aus dem Produkt- und Markenschutz, der mittels markenrechtlich geschützter und / oder kopiersicherer Kennzeichen arbeitet. Andererseits der Ansatz aus der Logistik, der mittels Tracking&Tracing Produkte und Güter auf ihrem Weg

durch die Supply-Chain verfolgt (siehe Abschnitt 1.2.2, S. 8 mit Abbildung 1-8, S. 11).

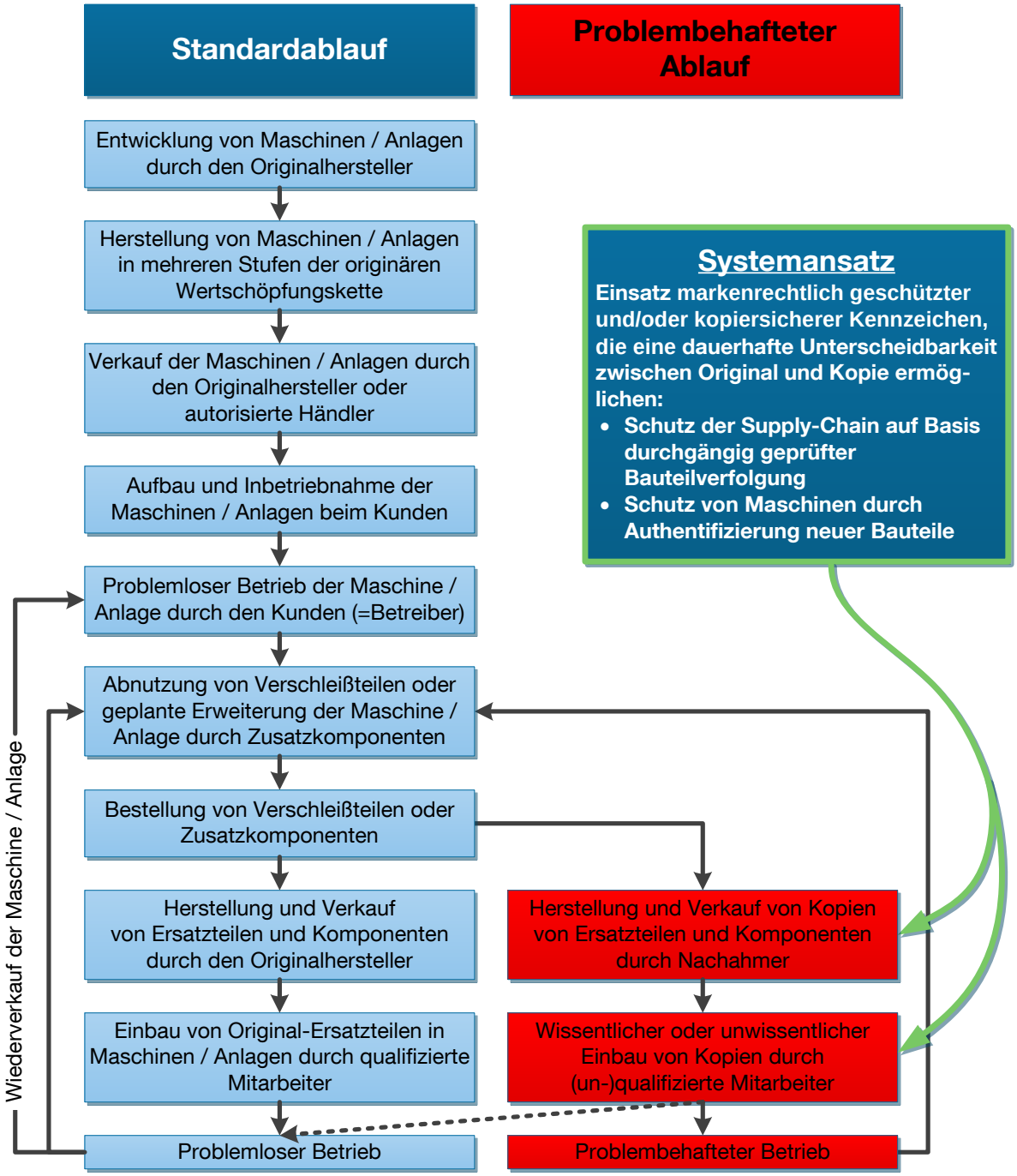


Abbildung 5-1: Standardablauf und problembehafteter Ablauf im Maschinen- und Anlagenbau und Ansatz des zu entwickelnden technischen Systems, in Anlehnung an [Abe-10 S. 97]

5.1 Referenzszenario

Betrachtet man die Supply-Chain eines Maschinen- und Anlagenbauers, so lassen sich vereinfacht die Stufen Herstellung, Vertrieb, Logistik und Kunde feststellen (siehe Abbildung 5-2, oben). Dabei können Kopien von Komponenten und Ersatzteilen auf jeder Stufe in die originäre Supply-Chain gelangen, wie *Günthner* bereits 2006 feststellt [Gün-06b]. Dies wird bestätigt durch eigene Recherchen [z. B. Akt-13, Die-08, Dri-07, Hun-06, Mak-13, Org-01 S. 32, Sto-13, Wal-05 S. 3, Wib-12, Win-13, ZDF-08] und Expertengespräche bei ausgewählten Unternehmen des Maschinen- und Anlagenbaus [Bra-08a, Dol-08, Pet-08, Rec-08].

Daher ist es sinnvoll, einerseits das Bauteil zu schützen und als Original erkennbar zu machen durch Mittel des Produkt- und Markenschutzes und andererseits die gesamte Supply-Chain zu schützen durch Ansätze des T&T (zu T&T siehe Abschnitt 3.2.1, S. 41). Sofern an jedem I-Punkt der Supply-Chain zusätzlich eine Authentifizierung stattfindet, können Kopien nicht unentdeckt in die originäre Supply-Chain eindringen und Kunden, deren Maschinen oder Anlagen, den Originalhersteller oder Vertriebspartner (be-)schädigen. Der I-Punkt der T&T-Systeme wird aufgewertet zum IP-Punkt (siehe Abbildung 5-2, unten).

In der vorliegenden Arbeit wird daher ein System entwickelt, das mit markenrechtlich geschützten oder kopiersicheren Kennzeichen eine dauerhafte Unterscheidbarkeit zwischen Original und Kopie ermöglicht. Mit der Einrichtung von IP-Punkten kann dann ausgeschlossen werden, dass Kopien in die Wertschöpfungs- und Logistikkette des Originalherstellers einsickern oder Kunden in ihren Maschinen und Anlagen unwissentlich Kopien benutzen. Dieses Gesamtsystem aus gekennzeichneten Bauteilen und IP-Punkten mit angeschlossener Datenarchivierung und -auswertung soll hier als technisches Produktpiraterie-Schutzsystem bezeichnet werden.

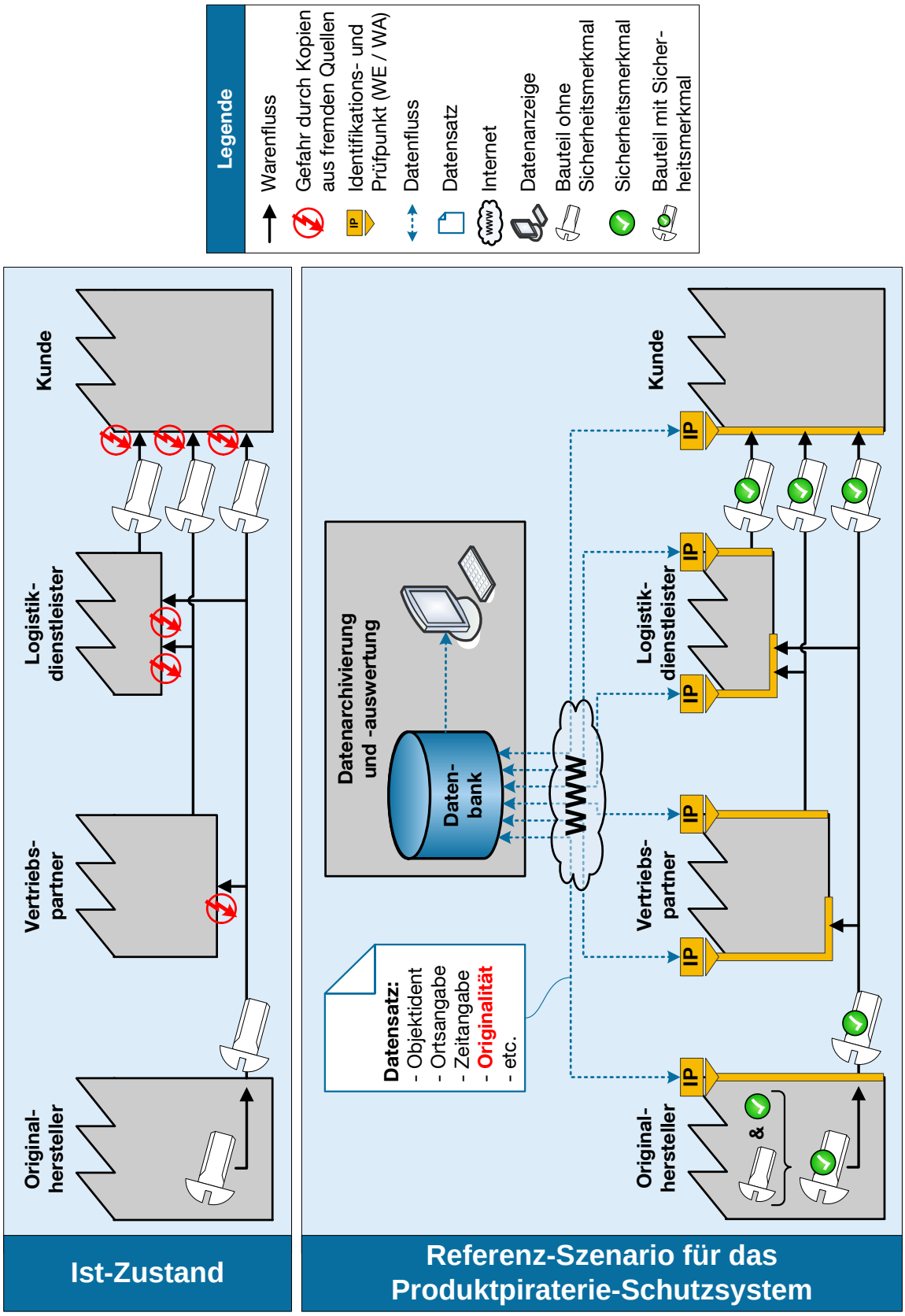


Abbildung 5-2: **Ist-Zustand sowie Referenzszenario für den Plan-Zustand**

5.2 Betroffene und schützenswerte Bauteile

In Abbildung 1-4, S. 6 wird deutlich, dass im Maschinen- und Anlagenbau insbesondere auch Komponenten und Ersatzteile sehr stark von Produktpiraterie betroffen sind. Die speziell betroffenen Bauteile der eigenen Maschinen und Anlagen sind den jeweiligen Herstellerunternehmen meist bekannt. Würde das jeweilige Unternehmen genau für diese betroffenen Bau- und Ersatzteile Maßnahmen im Sinne einer Kennzeichnung mit einem Sicherheitsmerkmal ergreifen, würde es in mehrfacher Hinsicht ungeschickt agieren, denn

- es könnten dabei auch Teile gekennzeichnet werden, die nur einen kleinen oder gar keinen Beitrag zum Jahreserfolg leisten und / oder auch für die Funktion der Maschinen und Anlagen von geringer Bedeutung sind und / oder auch für das Unternehmen keine wichtige Rolle spielen,
- der präventive Charakter der Gesamtmaßnahme ginge verloren, da speziell Bauteile aus Neuentwicklungen nicht berücksichtigt würden, da diese naturgemäß noch nicht von Produktpiraterie betroffen sind und für diese erst nach Auftauchen der ersten Kopien Maßnahmen ergriffen werden würden.

Würde das jeweilige Unternehmen hingegen alle Bauteile von Maschinen oder Anlagen als Originale oder gar Unikate kennzeichnen, wäre dies bei Weitem zu aufwendig und zu teuer.

Es ist aber aufgrund der generellen Struktur des Ersatzteilmarktes sehr schwierig, eine zielführende Einteilung der eigenen Komponenten und Teile vorzunehmen, denn „weltweite heterogene Märkte sowie eine Vielzahl an Ersatzteilen, Zulieferern, Kunden, Händlern und Wettbewerbern erschweren es den Originalherstellern zunehmend, eine transparente Bewertung der Pirateriegefährdung für die eigenen Ersatzteile zu treffen“ [Gün-11b S. 13]. Aus diesem Grund sind Kriterien zur Bestimmung von schützenswerten Bauteilen von zentraler Bedeutung.

5.2.1 Kriterien zur Auswahl von schützenswerten Bauteilen

Die schützenswerten Bauteile bilden eine Schnittmenge aus Bauteilen, welche für Originalhersteller wichtig und werthaltig sind, und Bauteilen, die für Nachahmer interessant sind (siehe Abbildung 5-3).

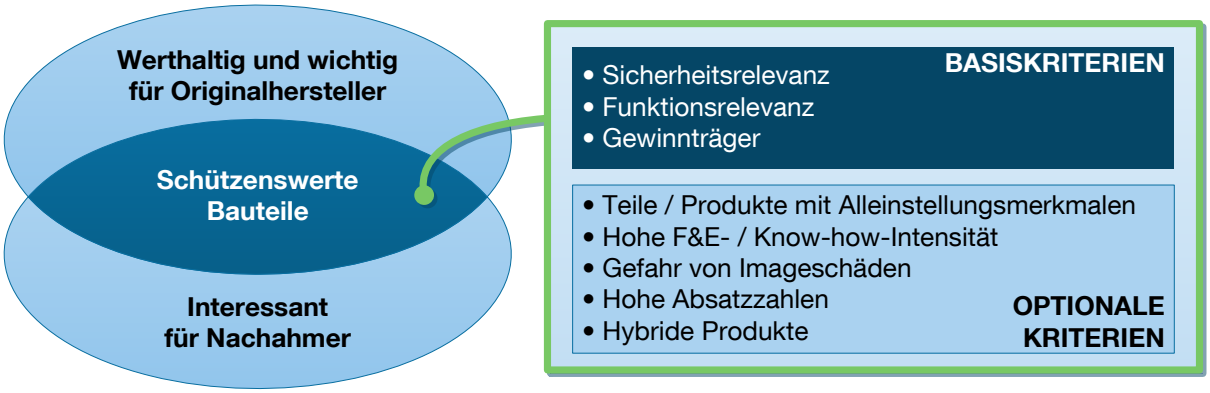


Abbildung 5-3: Auswahlkriterien für schützenswerte Bauteile

Um diese schützenswerten Bauteile zu bestimmen, dienen einerseits Basiskriterien und andererseits optionale Kriterien [in Anlehnung an die Vorveröffentlichung durch den Autor in Sto-12]. Als Basiskriterien können eingestuft werden:

- Sicherheitsrelevanz:
  Haben Bauteile eine hohe Relevanz bezüglich der Sicherheit der Gesamtmaschine, sollte eine eingehende Prüfung erfolgen, ob diese Bauteile präventiv als Originale zu kennzeichnen sind – dies insbesondere im Vorgriff auf etwaige Fälle mit Schäden für Leib und Leben bei Maschinenbedienern oder Dritten, in denen vor Gericht der Nachweis erbracht werden muss, dass die Fehlfunktion nicht durch Originalbauteile verursacht wurde.
- Funktionsrelevanz:
  Bauteile, die eine zentrale Rolle für die Funktionsfähigkeit einer Maschine / Anlage innehaben, sind daraufhin zu prüfen, ob diese Bauteile präventiv als Originale zu kennzeichnen sind. Insbesondere bei Verfügbarkeits- und Funktionsgarantien gegenüber dem Kunden könnte dann im Streitfall einfach nachgewiesen werden, dass Funktionsstörungen nicht durch Originalbauteile verursacht wurden.
- Gewinnträger:
  Komponenten und Ersatzteile spielen für den Unternehmensgewinn im Maschinen- und Anlagenbau eine gewichtige Rolle (siehe Abschnitt 1.1.2, S. 2). Daher sollten Bauteile, die einen großen Beitrag zum Unternehmenserfolg erbringen, präventiv als Originale gekennzeichnet werden, um eine Unterscheidung gegenüber Kopien zu ermöglichen.

Als optionale Kriterien zur Bestimmung schützenswerter Bauteile können genannt werden:

- Teile / Produkte mit Alleinstellungsmerkmal:
  Bauteile und Produkte, die gegenüber den Wettbewerbern ein Alleinstellungsmerkmal darstellen, können gekennzeichnet werden, um eine klare Unterscheidbarkeit gegenüber Kopien zu ermöglichen und diesen Unterschied klar deutlich zu machen.
- Hohe F&E- / Know-how-Intensität:
  Bestimmte Elemente von Maschinen und Anlagen bedürfen großer Investitionen in Forschung und Entwicklung (F&E) und beinhalten somit umfangreiches Know-how. Diese Elemente können mit dem Ziel der Vorbeugung vor Kopieren und zur Sicherstellung der Originalität mit entsprechenden Sicherheitsmerkmalen versehen werden.
- Gefahr von Imageschäden:
  Bei Bauteilen, bei deren Fehlfunktion oder Versagen ein großer Imageschaden für den Originalhersteller zu befürchten ist, können zur klaren Unterscheidung gegenüber Kopien mit Sicherheitsmerkmalen als Originale gekennzeichnet werden.
- Hybride Produkte:
  Es gibt Komponenten und Ersatzteile, die als hybride Produkte in Verknüpfung mit einer Dienstleistung angeboten werden, deren Wert für den Kunden durch die Integration den Wert der Teilleistungen übersteigt [Böh-06 S. 83]. Um sicher zu stellen, dass die jeweilige Dienstleistung nur erbracht wird, wenn ein Kunde ein Originalteil im Einsatz hat, können die betreffenden Teile als Originale gekennzeichnet werden.

5.2.2 Beispiele für schützenswerte Bauteile

Dieses Vorgehen zur Bestimmung von schützenswerten Bauteilen konnte gemeinsam mit den Beispielunternehmen Homag Group AG, Multivac Sepp Haggenmüller GmbH & Co. KG und Vollmer Werke Maschinenfabrik GmbH validiert werden. Als Ergebnis wurden somit die folgenden Bauteile aufgrund der in Abbildung 5-3 genannten Kriterien identifiziert [siehe auch die Vorveröffentlichung des Autors in Gün-11c].

	Schützenswerte Bauteile	Basiskriterien			Optionale Kriterien				
		Sicherheitsrelevanz	Funktionsrelevanz	Gewinnträger	Teile / Produkte mit Alleinstellungsmerkmal	Hohe F&E-/Know-how-Intensität	Gefahr von Imageschäden	Hohe Absatzzahlen	Hybrides Produkt
Homag	Aggregate / HSK-Schnittstelle 	✘	✘	✘	(✘)	✘			
	Kettenplatten 		✘	✘		✘		✘	
	Schmierstoff 			✘				✘	
Multivac	Klammerkette 		✘			✘	✘		
	Siegeldichtung 		✘			✘	✘		
Vollmer	Drahttransportrolle 		✘			✘			
	Einmesslehre 		✘						

Abbildung 5-4: Beispiele für schützenswerte Bauteile (Bildquellen Bauteile: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, Vollmer Werke Maschinenfabrik GmbH)

In Abbildung 5-4 wird deutlich, dass Ersatzteile und Komponenten unterschiedlichster Art betroffen und verbindende Eigenschaften oder Elemente kaum zu bestimmen sind. Daher ist eine unternehmensindividuelle Auswahl der schützenswerten Bauteile mit Hilfe der in Abbildung 5-3 genannten Kriterien notwendig.

5.3 Strategisches Vorgehen zum Schutz schützenswerter Bauteile

Das legitime Ziel jedes Originalherstellers ist es, unter Beachtung des Gesetzes gegen Wettbewerbsbeschränkungen [GWB, BMJ-13a] und des Gesetzes gegen den

unlauteren Wettbewerb [UWG, BMJ-13b] Kopien eigener Bauteile möglichst zu vermeiden, um den eigenen erarbeiteten Wettbewerbsvorsprung zu erhalten. Zumindest jedoch sollte es eine klare Unterscheidbarkeit zwischen der Originalware und Kopien geben. Dies ist schon aufgrund dessen wichtig, da die Kopien von Bau- und Ersatzteilen oftmals ein so hohes Qualitätsniveau erreichen, dass die Unterscheidung selbst für Experten sehr schwierig ist (siehe Abbildung 5-5) [Kle-10 S. 8, Kro-06 S. 4, Sit-06, Win-07, Wil-07].

Abbildung 5-5: Original und Kopie (Bildquelle: APM - Aktionskreis gegen Produkt- und Markenpiraterie e.V.)

Hierfür ist ein logisch aufgebautes, methodisch unterstütztes, strategische geschicktes Vorgehen, das sämtliche Aspekte der Produkt- und Markenpiraterie im Maschinen- und Anlagenbau berücksichtigt, notwendig. Dieses Vorgehen wird in dieser Arbeit entwickelt – einen Überblick gibt Abbildung 5-6.

Die Basis für eine erfolgreiche Arbeit gegen unerwünschte Nachbauten und Kopien liegt, wie in Abschnitt 2.5 dargestellt, in der Anmeldung von Schutzrechten (siehe Tabelle 2-1, S. 25). Da jedoch Marken und sonstige Kennzeichen im Vergleich zu den übrigen Schutzrechten eine besondere Rolle einnehmen, ist der initiale Schritt zweigeteilt.

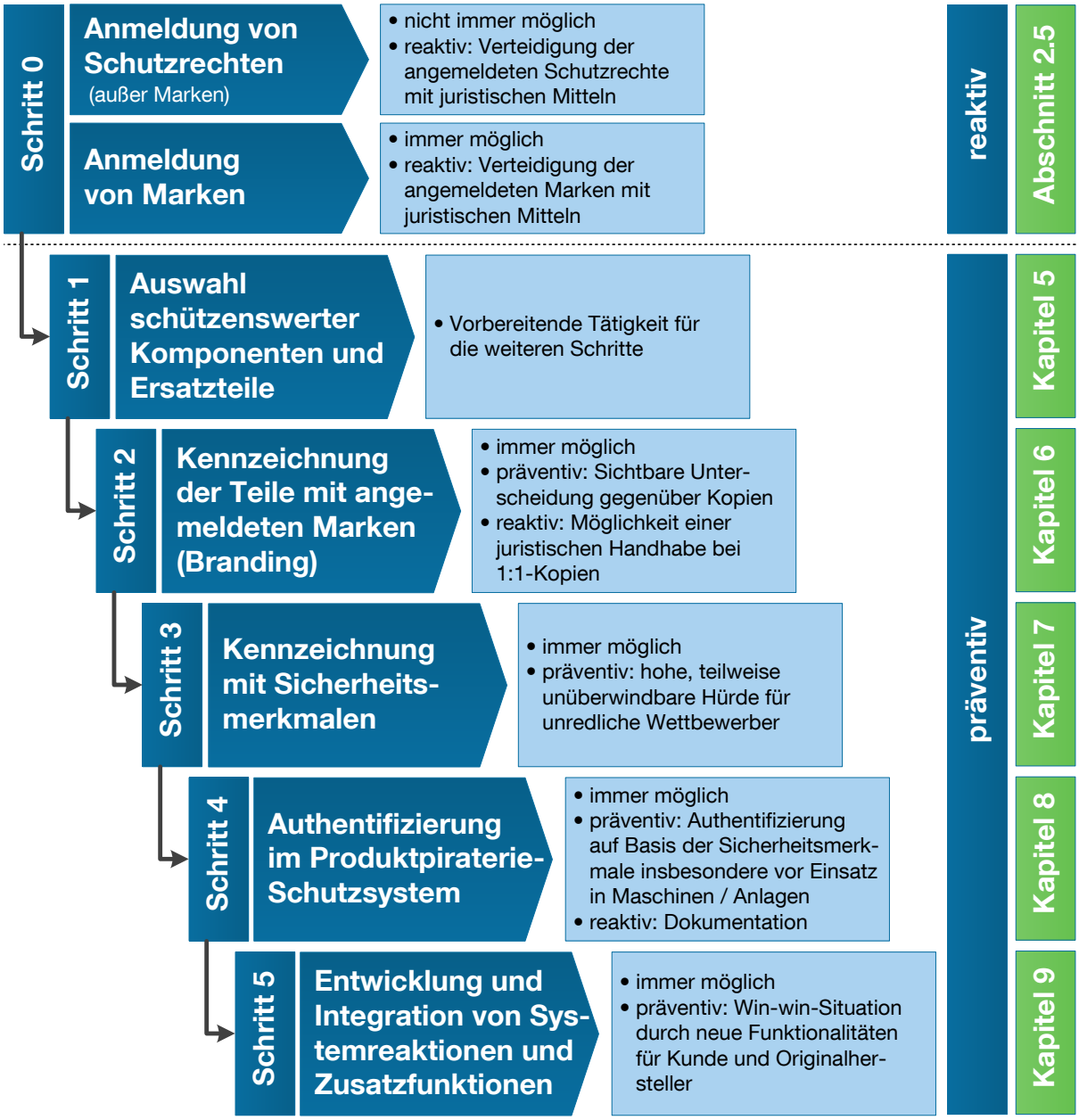


Abbildung 5-6: Strategisches Vorgehen

Die Anmeldung erzeugnis- oder teilebezogener Schutzrechte wie Geschmacksmuster, Gebrauchsmuster und Patente ist bei den Unternehmen bereits gängige Praxis. Gerade das Patent ist in Deutschland ausgesprochen beliebt [Pat-13]. Die Patentanmeldungen sind in den vergangenen Jahren stetig steigend [DPMA-13, EPO-13, Gra-13, Nee-07 S. 24]. Ein Patent kann jedoch nicht immer angemeldet werden, z. B. ist der Stand der Technik nicht patentierbar [DPMA-12]. Zudem kann mit diesen eingetragenen Schutzrechten lediglich reaktiv gearbeitet werden, wie in Abschnitt 2.5, S. 23 dargestellt. D. h. erst, wenn ein Verstoß gegen eines dieser Rechte durch einen unredlichen Wettbewerber erfolgt ist, können juristische Mittel zur Verteidigung eingesetzt werden. Neben dem reaktiven Charakter dieser Maßnahme gel-

ten alle weiteren in Abschnitt 2.5, S. 23 genannten Nachteile. Auch können im Falle der Erteilung eines Schutzrechts lediglich Erzeugnisse aus dem Ast „Pirateriewaren“ in Abbildung 2-2, S. 32 bekämpft werden. Nachahmungen, Graumarktware und Waren aus der Dritten Schicht bleiben durch diese Maßnahme unberührt bzw. unentdeckt.

Bei der Anmeldung von Marken und sonstigen Kennzeichen (siehe Tabelle 2-1, S. 25) handelt es sich ebenfalls um ein Schutzrecht und kann im Gegensatz zu den anderen Schutzrechten und unter Berücksichtigung bereits bestehender und angemeldeter Marken immer erfolgen. Die Anmeldung der Marken ist in den Produktions- und Vertriebsländern wichtig, insbesondere aber auch in den Ländern, in denen Fälschungen hergestellt und verkauft werden [Wel-07 S. 61]. Die besondere Rolle der Marken besteht darin, dass die Etablierung und Verteidigung starker Marken eine wesentliche Komponente im Kampf gegen Produkt- und Markenpiraterie darstellt [Fuc-06 S. 335 ff.].

Nachdem ein Unternehmen mit den in Abbildung 5-6, „Schritt 0“ genannten Anmeldungen verschiedener Schutzrechte eine solide juristische Basis für eine erfolgreiche Arbeit gegen Produkt- und Markenpiraterie gelegt hat, und in „Schritt 1“ seine schützenswerten Bauteile und Komponenten bestimmt hat, beginnt mit „Schritt 2“ die geschickte Verwendung und konsequente Nutzung dieser Rechte mittels präventiver Kennzeichnung der in Abschnitt 5.2, S. 87 ausgewählten schützenswerten Komponenten und Bauteile. Zunächst können die angemeldeten Marken als einfaches Kennzeichen verwendet werden, um eigene Erzeugnisse mit diesen Marken zu kennzeichnen und so eine einfache Unterscheidung zwischen Original und Kopie zu erzeugen. Eine genaue Beschreibung erfolgt im Kapitel „6 Branding: Kennzeichnung schützenswerter Komponenten und Ersatzteile mit unternehmenseigenen Marken“, S. 101.

Die Wirkung dieser Form der Kennzeichnung besteht im juristischen Schutz der angemeldeten Marken. Ein Wettbewerber darf aus rechtlichen Gründen das Markenzeichen bei der Erzeugung eines Konkurrenzproduktes oder einer Kopie nicht mitkopieren. Das auf einem Produkt sichtbare Markenzeichen stellt somit eine erste Hürde dar und wirkt damit präventiv. Sollte ein Kopist ein Erzeugnis eins zu eins, also mit Markenzeichen kopieren, ist dies ein Verstoß gegen das Markenrecht. Die Verteidigung des eingetragenen Schutzrechts mit juristischen Mitteln ist somit als Reaktion auf den Verstoß direkt möglich. Mit diesem ersten kennzeichnenden Ele-

ment der Gesamtstrategie kann somit gegen alle Arten von Kopien gearbeitet werden – insbesondere auch gegen Nachahmungen (siehe Abbildung 2-2, S. 32).

Bei der reinen Verwendung von Marken als Kennzeichen auf Originalbauteilen besteht die Gefahr, dass ein unredlicher Wettbewerber Kopien herstellt und das Markenzeichen rechtswidrig mitkopiert. Die Hürde ist zwar wesentlich höher, als bei nicht-gebrandeten Bauteilen, aber auszuschließen ist es nicht. Sehr gute Kopien können dann den Originalen täuschend ähnlich sehen. Zwar ist im Zweifel die Kopie spätestens unter Einsatz von Labortechnik vom Original unterscheidbar, aber die ursprünglich präventive Wirkung der Kennzeichnung mit einer Marke geht in diesem Fall verloren.

Daher kommen im „Schritt 3“ zusätzlich zu den verwendeten Markenzeichen auf den ausgewählten schützenswerten Komponenten und Bauteilen Sicherheitsmerkmale zum Einsatz, welche die Teile jederzeit zweifelsfrei als Originale oder sogar als Unikate erkennbar machen. Da Sicherheitsmerkmale kopiersicher sind (siehe Abschnitt 2.7.1, S. 27), bleiben die Originalwaren permanent gegenüber Kopien unterscheidbar. Der Einsatz passender Sicherheitsmerkmale ist aufgrund des breiten Angebots und der Vielzahl verschiedener Technologien nahezu immer möglich. Eine Übersicht und Einordnung existierender Technologien befindet sich in Abschnitt 3.1, S. 37 und Anhang A, ein methodisches Vorgehen zur Auswahl passender Sicherheitsmerkmale je schützenswertem Bauteil wird in Kapitel 7, S. 105 entwickelt.

Die präventive Wirkung ist bei sichtbaren Sicherheitsmerkmalen offensichtlich. Eine Eins-zu-eins-Kopie eines Produkts ist aufgrund des für alle Beteiligten erkennbaren Sicherheitsmerkmals nicht möglich. Original und Kopie sind immer direkt unterscheidbar. Bei unsichtbaren Sicherheitsmerkmalen wirkt deren Einsatz auf andere Weise präventiv im Moment der ersten Prüfung. Dort wird das kopierte Erzeugnis nicht als Original bestätigt und kann noch vor dem ersten Einsatz in einer Maschine oder Anlage einer genaueren Überprüfung unterzogen werden.

Dafür werden in „Schritt 4“ an den relevanten Stellen im Wertschöpfungs- und Logistiknetz entsprechende IP-Punkte eingerichtet. Die datentechnische Verknüpfung der verteilt im Netzwerk eingerichteten IP-Punkte lässt ein technisches Produktpiraterie-Schutzsystem entstehen, das analog zu T&T-Systemen arbeitet (siehe Abschnitt 3.2.1, S. 41 mit Abbildung 3-1, S. 43). Das Produktpiraterie-Schutzsystem kann neben den T&T-Funktionalitäten aber zusätzlich auch sämtliche Objekte auf ihre Originalität hin überprüfen, wie dies in der Zielstellung und im Referenzszenario

bereits formuliert ist (siehe Abschnitt 1.2.2, S. 8 und Abschnitt 5.1 mit Abbildung 5-2). Ein wichtiges Element des Produktpiraterie-Schutzsystems ist die Erzeugung von Prüfdatensätzen bei jeder erfolgten Überprüfung an einem IP-Punkt und deren Dokumentation zur Auswertung sowie für spätere Nachweise. Nur ein solches System kann sämtliche Ausprägungen möglicher Kopien von Originalwaren unterscheiden und darüber hinaus auch Graumarktware und Produkte aus der Dritten Schicht erkennen, entsprechende Systemreaktionen auslösen und damit gegen alle Formen der Produkt- und Markenpiraterie wirken (siehe Abbildung 2-2, S. 32). Das Konzept für ein solches System wird in Kapitel 8, S. 179 erarbeitet.

Zur Vervollständigung der Strategie werden im „Schritt 5“ passende Systemreaktionen integriert sowie neue Funktionen entwickelt. Diese werden erst durch den Einsatz von Sicherheitsmerkmalen auf Komponenten und Teilen sowie die Einrichtung der IP-Punkte im gesamten Produktpiraterie-Schutzsystem ermöglicht. Die Reaktionen und Funktionen sollen dem Originalhersteller und insbesondere auch dem Kunden einen Mehrwert bieten, der nur unter dem Einsatz von Originalbauteilen möglich ist. Die Systemreaktionen erfolgen aufgrund des Prüfergebnisses meist in informierender Form. Die Zusatzfunktionen reichen von einer automatischen Bauteilidentifikation auf Maschinen und Anlagen und einer automatischen Übergabe bauteilspezifischer Betriebsparameter über eine Nachverfolgbarkeit der Ersatzteile auf dem Transportweg bis hin zu einer Verschleißerkennung und einer damit verbundenen Reduktion der Lagerkosten für Ersatzteile durch optimales Ersatzteilmanagement. Diese Zusatznutzen sind abhängig vom eingesetzten Sicherheitsmerkmal und wirken präventiv. Denn ein Kunde, der von den neuen Zusatzfunktionen direkt profitiert, wird weiterhin Originalbauteile einsetzen wollen. Die Zusatznutzen werden in Kapitel 9, S. 215 dargestellt.

5.4 Anforderungen an Sicherheitsmerkmale und das Produktpiraterie-Schutzsystem

Um das Ziel einer dokumentierten Authentifizierung für Bauteile des Originalherstellers zu erreichen, ergeben sich Anforderungen aus den beiden Ansätzen des T&T sowie des Produkt- und Markenschutzes (siehe Abschnitt 5.1). Aus dem Produkt- und Markenschutz lassen sich die in Abschnitt 5.4.1 aufgeführten „Anforderungen an Sicherheitsmerkmale“ ableiten. Aus dem Tracking&Tracing ergeben sich die in

Abschnitt 5.4.2 genannten „Anforderungen an ein System zur dokumentierten Authentifizierung schützenswerter Bauteile mittels Sicherheitsmerkmalen“.

5.4.1 Anforderungen an Sicherheitsmerkmale

In Anlehnung an die *Internationale Handelskammer* (ICC: International Chamber of Commerce) sowie *Winkler und Wang* lassen sich allgemeine Anforderungen an Sicherheitsmerkmale des Produkt- und Markenschutzes formulieren [ICC-06 S. 9, Win-07 S. 210]:

- Eindeutigkeit:
  Das Sicherheitsmerkmal muss das Objekt eindeutig als Original erkennbar machen, d. h. ein Sicherheitsmerkmal darf weltweit nicht zufällig mehrfach existieren.
- Fälschungssicherheit:
  Das Sicherheitsmerkmal darf nur mit größtmöglichem Aufwand und Kosten von Dritten nachgeahmt werden können. Auch soll es nicht nachträglich anbringbar, sondern möglichst fester Bestandteil des Produktes sein.
- Dauerhaftigkeit:
  Das Sicherheitsmerkmal soll während des gesamten Produktlebenszyklus vorhanden und nicht (spurenfrei) entfernbar oder übertragbar auf andere Produkte sein, um eine dauerhafte Authentifizierung zu gewährleisten.
- Wirtschaftlichkeit:
  Der Einsatz des Sicherheitsmerkmals soll wirtschaftlich sein. Dies beinhaltet auch die einfache Anbringung sowie schnelle und einfache Authentifizierung.

5.4.2 Anforderungen an ein System zur dokumentierten Authentifizierung schützenswerter Bauteile mittels Sicherheitsmerkmalen

Der Schutz des gesamten Wertschöpfungsnetzwerks eines Originalherstellers lässt sich aus den Überlegungen in Abschnitt 5.1 motivieren. Zusätzlich ist klar, dass die Sicherheit für Originalwaren, die mit Sicherheitsmerkmalen gekennzeichnet sind, weiter erhöht werden kann, wenn diese innerhalb des gesamten Netzes mittels des zu entwickelnden technischen Produktpiraterie-Schutzsystems verfolgt werden (siehe Abschnitt 5.1 mit Abbildung 5-2). Die Kontrolle an den speziell ausgerüsteten IP-Punkten mit integrierter Authentifizierung erzeugt gleichzeitig ein digitales Abbild des Wegs eines Bauteils innerhalb des Wertschöpfungsnetzwerks und ermöglicht eine

detaillierte Überprüfung der Herkunft. Dies lässt Rückschlüsse auf den Verbleib des Produktes und somit auf etwaige Störungen im Netzwerk zu, z. B. die Feststellung, ob ein Produkt zeitgleich bei verschiedenen Kunden als Original authentifiziert wurde.

Zudem werden Nicht-Originale an den Authentifizierungspunkten direkt erkannt, da alle Formen von Kopien, Graumarktwaren und Waren aus der Dritten Schicht (siehe Abbildung 2-2, S. 32) keine oder nicht die passenden Sicherheitsmerkmale tragen. Somit kann das gesamte originale Wertschöpfungs- und Logistiknetzwerk gegen das Eindringen von Nicht-Originalwaren geschützt werden. Als Anforderungen an das skizzierte System lassen sich somit feststellen:

- Offenes, skalierbares System zum einfachen Aufschalten beliebig vieler Instanzen:
    - Beliebig viele Originalhersteller mit beliebig vielen Bauteilen und Komponenten (Maschinen- und Anlagenhersteller)
    - Beliebig viele IP-Punkte bei den Beteiligten der originalen Wertschöpfungs- und Logistikkette (Maschinen- und Anlagenhersteller, Kunden als Maschinen- und Anlagenbetreiber, Vertriebspartner, Logistikdienstleister, Wartungsfirmen, etc.)
- Offenes System zur Integration beliebiger verschiedener Sicherheitsmerkmale als Kennzeichnungs- und Authentifizierungstechnologien zum Schutz der gesamten originalen Wertschöpfungs- und Logistikkette gegen Eindringen von Nicht-Originalwaren im Sinne von Abbildung 2-2, S. 32
- Unternehmensübergreifend konsistentes Datenmodell zum durchgängigen Datenaustausch
- Möglichkeit der Zusammenführung und Ausgabe der freigegebenen Daten für alle berechtigten Beteiligten zu einer Originalware (Tracking&Tracing-Daten sowie Prüfergebnisse)
- Anzeige passender systemseitiger Reaktionen lokal am IP-Punkt, aber auch aus der zentralen Sicht und der Auswertung aller Daten zu einem Bauteil / einer Maschine
- Sicheres Hosting der Daten und sicherer Datenaustausch

Neben diesen Anforderungen, die sich aus der Verwendung eines adaptierten T&T-Systems ergeben, gibt es weitere Anforderungen an das technische Produktpiraterie-Schutzsystem. Diese weiteren Anforderungen konnten in Zusammenarbeit mit

ausgewählten Unternehmen des Maschinen- und Anlagenbaus in Expertengesprächen ermittelt werden [z. B. Bra-08a, Dol-08, Pet-08, Rec-08].

Dem Originalhersteller einer Maschine oder Anlage entgeht beim Einsatz von kopierten Bauteilen oder Komponenten nicht nur Umsatz und Gewinn. Bei Funktionsstörungen in der Maschine oder Anlage aufgrund des Einsatzes kopierter Teile entsteht für den Hersteller, der dem Kunden vertraglich Funktions- und Verfügbarkeitsgarantien zusichert und für seine Produkte haftet, zusätzlich eine Situation, die äußerst schwierig zu bewältigen ist [Dol-10]. Um dem vorzubeugen, ist es ideal, wenn eine Maschine oder Anlage bei einem Neustart eingebaute schützenswerte Bauteile automatisch auf Originalität überprüfen und adäquat reagieren kann. So kann die Originalität von eingebauten Teilen sichergestellt und dem Maschinenbediener angezeigt werden [Gün-11d]. Daraus ergeben sich folgende maschinenbezogene Anforderungen an das System zur dokumentierten Authentifizierung schützenswerter Bauteile:

- Authentifizierung eingebauter schützenswerter Bauteile in der Maschine vor bzw. während des Maschinenstarts
- Möglichkeit der Online-Authentifizierung und Möglichkeit der Offline-Authentifizierung zur Realisierung verschiedener Sicherheitslevel
- automatische, halbautomatische oder manuelle Authentifizierung eingebauter schützenswerter Bauteile – abhängig des gewünschten Sicherheitsmerkmals und Sicherheitslevels
- sofortige Mitteilung des Prüfergebnisses am IP-Punkt
- Lokale Speicherung des Prüfergebnisses zur Einsicht der Historie für einen Bediener am IP-Punkt
- Möglichkeit der Übertragung des Prüfergebnisses in eine zentrale Datenbank bei einer Freigabe durch den Betreiber des IP-Punkts
- Möglichkeit der Zusammenführung und Visualisierung der freigegebenen Prüfergebnisse zu einer Maschine / Anlage für alle berechtigten Beteiligten zur Darstellung der aktuellen Bestückung einer Maschine
- Möglichkeit der Integration von systemergänzenden kundenorientierten Dienstleistungen und Zusatzfunktionen zur Generierung einer Win-win-Situation für alle Beteiligten

5.4.3 Zusammenfassung der Anforderungen an das Produktpiraterie-Schutzsystem

Für eine bessere Übersicht und für eine klare Referenzierung innerhalb der Arbeit werden diese Anforderungen in einer Anforderungsliste erfasst [nach Lin-09 S. 108]:

Tabelle 5-1: Anforderungsliste für ein System zur dokumentierten Authentifizierung schützenswerter Bauteile mittels Sicherheitsmerkmalen

Nr.			Beschreibung
1			**Anforderungen an Sicherheitsmerkmale**
	1.1		**Eindeutigkeit:** Das Sicherheitsmerkmal muss das Objekt eindeutig als Original erkennbar machen, d.h. ein Sicherheitsmerkmal darf weltweit nicht zufällig mehrfach existieren.
	1.2		**Fälschungssicherheit:** Das Sicherheitsmerkmal darf nur mit größtmöglichem Aufwand und Kosten von Dritten nachgeahmt werden können. Auch soll es nicht nachträglich anbringbar, sondern möglichst fester Bestandteil des Produktes sein.
	1.3		**Dauerhaftigkeit:** Das Sicherheitsmerkmal soll während des gesamten Produktlebenszyklus vorhanden und nicht (spurenfrei) entfernbar oder übertragbar auf andere Produkte sein, um eine dauerhafte Authentifizierung zu gewährleisten.
	1.4		**Wirtschaftlichkeit:** Der Einsatz des Sicherheitsmerkmals soll wirtschaftlich sein. Dies beinhaltet auch die einfache Anbringung sowie schnelle und einfache Authentifizierung.
2			**Anforderungen an ein System zur dokumentierten Authentifzierung**
	2.1		**Identifikations- und Prüfpunkte:**
		2.1.1	Integration beliebiger existierender oder neuer Sicherheitsmerkmale
		2.1.2	Online- und Offline-Authentifizierung möglich
		2.1.3	Unmittelbare Mitteilung des Prüfergebnisses an den Prüfer
		2.1.4	Passende systemseitige Reaktion lokal am IP-Punkt
		2.1.5	Lokale Speicherung des Prüfergebnisses zur Einsicht der Historie
		2.1.6	Möglichkeit der Übertragung des Prüfergebnisses in eine zentrale Datenbank bei einer Freigabe durch den Maschinenbetreiber
		2.1.7	IP-Punkte in einer Maschine / Anlage zur Authentifizierung eingebauter schützenswerter Bauteile in einer Maschine / Anlage beim Maschinenstart
		2.1.8	Automatische, halbautomatische oder manuelle Authentifizierung eingebauter schützenswerter Bauteile
	2.2		**Gesamtsystem:**
		2.2.1	Beliebig viele Originalhersteller mit beliebig vielen Bauteilen und Komponenten
		2.2.2	Beliebig viele IP-Punkte in der originalen SC
		2.2.3	Möglichkeit der Datenübertragung der freigegebenen Daten in ein zentrales System
		2.2.4	Möglichkeit der Integration von systemergänzenden kundenorientierten Dienstleistungen und Zusatzfunktionen zur Generierung einer Win-win-Situation für alle Beteiligten
		2.2.5	Sicheres Hosting der Daten
		2.2.6	Sicherer Datenaustausch
	2.3		**Datenmodell:** Unternehmensübergreifend konsistent für durchgängigen Datenaustausch
	2.4		**Auswertung:**
		2.4.1	Zusammenführung, Auswertung und Ausgabe der freigegebenen Daten zu einer Originalware
		2.4.2	Zusammenführung, Auswertung und Ausgabe der freigegebenen Daten zu einer Maschine
		2.4.3	Passende systemseitige Reaktionen aus der zentralen Sicht und der Auswertung aller Daten zu einem Bauteil / einer Maschine

6 Branding: Kennzeichnung schützenswerter Komponenten und Ersatzteile mit unternehmenseigenen Marken

Im strategischen systematischen Vorgehen für Unternehmen zum Einsatz von Kennzeichnungs- und Authentifizierungstechnologien als präventive Maßnahmen gegen Produkt- und Markenpiraterie ist in „Schritt 2“ die Verwendung von unternehmenseigenen Marken und sonstigen Kennzeichen auf den Originalprodukten vorgesehen (siehe Abschnitt 5.3, S. 90 mit Abbildung 5-6, S. 92). Die Anmeldung von Marken in international bedeutenden Märkten erfolgt ohnehin aus Marketinggründen des jeweiligen Unternehmens. Die Nutzung dieses gewerblichen Schutzrechts durch die Abbildung des Markenzeichens auf Bauteilen liegt daher sehr nahe. Wie bei Konsumgütern stellt dieses Markenzeichen für Kunden auch ein Qualitätsmerkmal dar und hebt die eigenen Produkte aus der Masse gleichartiger Produkte heraus.

Das Abbilden von Marken und Markenzeichen ist ein Teilbereich des sogenannten Brandings, das neben dem Markieren auch die Gestaltung von Markennamen und Markenlogo sowie die Gestaltung von Produkt und Verpackung umfasst [Ste-11b S. 5, S. 69]. Diese Inhalte sind Gegenstand der Untersuchungen eines eigenen Themenfelds in der Wissenschaft, so dass hierzu zahlreiche Veröffentlichungen existieren [z. B. Bae-11, Dom-05, Esc-05, Esc-12, Mef-13, Per-11]. In dieser Arbeit wird lediglich die Verwendung der angemeldeten Marken auf den eigenen Originalbauteilen, deren Wirkung und Defizite kurz dargestellt.

Die Anbringung von unternehmenseigenen Marken und Markenzeichen auf Originalbauteilen kann auf unterschiedliche Weise erfolgen (siehe Abbildung 6-1). Beispielsweise kann das Markenzeichen mit Hilfe eines Etiketts aufgebracht werden. Vor Übertragen geschützt jedoch sind die Möglichkeiten der Integration in beispielsweise die Spritzgussform für Bauteile oder auch das Laserbeschriften.

Abbildung 6-1: Originalbauteile und -waren mit Markenzeichen (Quelle: HOMAG Holzbearbeitungssysteme GmbH)

Die Wirkung im Kontext Produkt- und Markenpiraterie ist sehr einfach: Ein redlicher oder auch ein unredlicher Wettbewerber darf aus rechtlichen Gründen das Markenzeichen bei der Erzeugung einer Kopie nicht mitkopieren. Die äußere Sichtbarkeit des Markenzeichens an einem Produkt stellt somit eine erste Hürde dar und wirkt bereits bei der Überlegung eine Kopie herzustellen präventiv. Die Unterscheidbarkeit zwischen Original und Kopie ist für alle Wirtschaftsbeteiligten leicht erkennbar.

Sollte ein Kopist ein Erzeugnis eins zu eins, also mit Markenzeichen kopieren, ist dies ein Verstoß gegen das Markenrecht. Die Verteidigung des eingetragenen Schutzrechts mit juristischen Mitteln ist somit als Reaktion auf den Verstoß direkt

möglich (siehe Abschnitt 2.5, S. 23 mit Abbildung 2-1, S. 23). Mit diesem ersten kennzeichnenden Element der Gesamtstrategie kann somit gegen alle Arten von Kopien gearbeitet werden – insbesondere auch gegen Nachahmungen (siehe Abbildung 2-2, S. 32).

Die ausschließliche Verwendung von Markenzeichen hat allerdings das Defizit, dass bei sehr guten, qualitativ sehr hochwertigen Eins-zu-Eins-Kopien, bei denen auch das Markenzeichen mitkopiert wird, der Nachweis der Nicht-Originalität der Kopie sehr schwierig ist. Um in diesem Fall auch bei juristischen Auseinandersetzungen erfolgreich zu sein, muss die Kopie zweifelsfrei als solche nachgewiesen werden können, was zwar meist mit labortechnischen Untersuchungen gelingt, der präventive Charakter der Maßnahme allerdings geht damit verloren. Zudem bleibt das Kennzeichnen mit Marken bei Graumarktwaren und Waren aus der Dritten Schicht ohne Wirkung. Daher ist es ratsam, auch mit Sicherheitsmerkmalen zu arbeiten und diese auf Originalwaren zur Anwendung zu bringen.

7 Kennzeichnung schützenswerter Komponenten und Ersatzteile mit Sicherheitsmerkmalen

Nach der Bestimmung der schützenswerten Komponenten und Ersatzteile von Maschinen oder Anlagen eines herstellenden Unternehmens nach den Kriterien in Abschnitt 5.2.1, S. 87 und der Anbringung eines Markenzeichens wie in Kapitel 6, erfolgt in diesem Kapitel die Auswahl der für diese Bauteile passenden Sicherheitsmerkmale. Dies entspricht im strategischen Vorgehen aus Abschnitt 5.3 „Schritt 3“ (siehe Abbildung 5-6, S. 92).

Zudem werden in diesem Kapitel dargestellt, wie Originalitäts- und Identitätskennzeichen zu einem Unikatkennzeichen kombiniert werden können, wie RFID als Sicherheitsmerkmal eingesetzt werden kann und wie die ausgewählten Sicherheitsmerkmale auf oder in Bauteile auf- oder eingebracht werden können.

Die Auswahl passender Sicherheitsmerkmale erfolgt sequenziell, indem für jedes schützenswerte Bauteil das nachfolgend dargestellte, neu entwickelte, methodische Vorgehen durchlaufen wird. Das Ergebnis sind ein oder auch mehrere passende Sicherheitsmerkmale je schützenswertem Bauteil.

Die Auswahl erfolgt in zwei Teilschritten. Im ersten Teilschritt wird eine Menge an prinzipiell möglichen Sicherheitsmerkmalen auf Basis technischer Rahmenbedingungen bestimmt. Im zweiten Teilschritt erfolgt mit einer wirtschaftlichen Bewertung eine weitere Einschränkung auf eine kleine Menge an für ein schützenswertes Bauteil passenden Sicherheitsmerkmalen (siehe Abbildung 7-1).

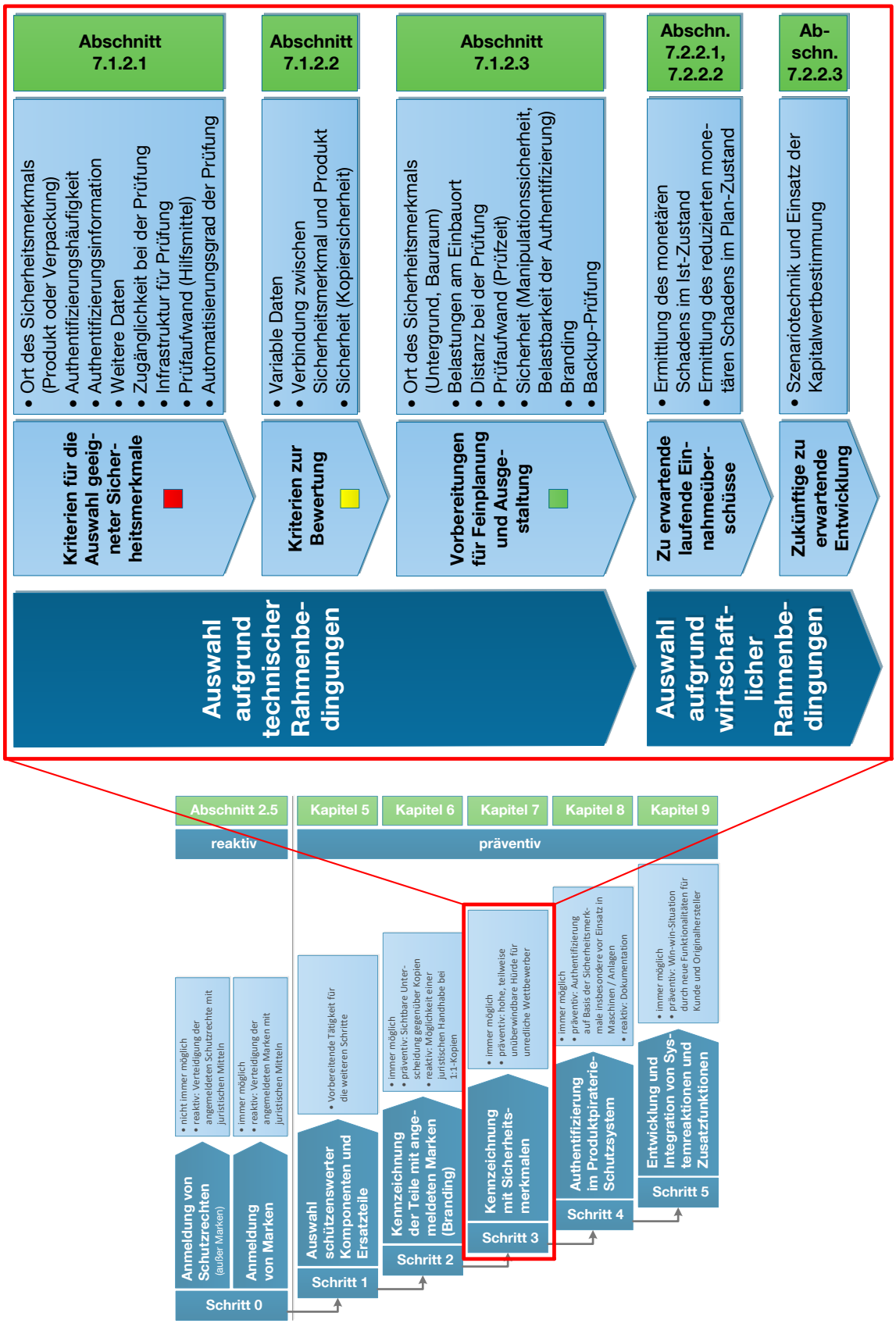


Abbildung 7-1: Vorgehen zur Auswahl passender Sicherheitsmerkmale im Kontext des strategischen Vorgehens aus Abbildung 5-6, S. 92

7.1 Auswahl von Sicherheitsmerkmalen aufgrund technischer Rahmenbedingungen

Die Auswahl möglicher Sicherheitsmerkmale aufgrund gegebener technischer Rahmenbedingungen basiert auf einem Abgleich zwischen

- den technischen Anforderungen durch das Bauteil und dessen Umgebung in der Herstellung und beim Einsatz in der Maschine und
- den technischen Eigenschaften von Sicherheitsmerkmalen.

Um diese Schlüssel-Schloss-Beziehung abzubilden, sind Kriterien mit entsprechenden Ausprägungen notwendig. Diese Kriterien müssen beide Sichtweisen – Eigenschaften von Sicherheitsmerkmalen sowie technische Anforderungen des schützenswerten Bauteils – sinnvoll abbilden und in einer Auswahlmethodik verwendet werden (siehe Abbildung 7-2).

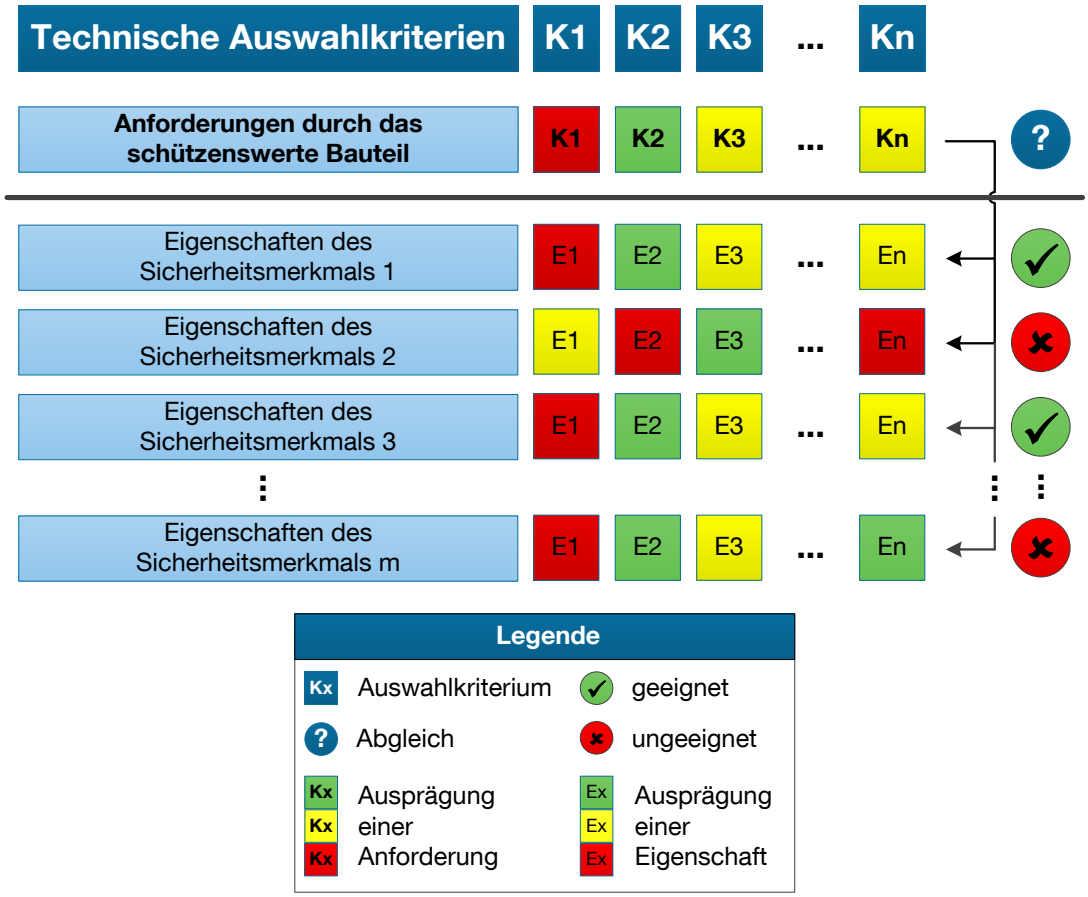


Abbildung 7-2: Schlüssel-Schloss-Prinzip bei der Bestimmung der passenden Sicherheitsmerkmale auf Basis technischer Auswahlkriterien

7.1.1 Technische Auswahlkriterien

Eine umfangreiche Liste an möglichen technischen Kriterien konnte in Zusammenarbeit mit Beispielunternehmen aus dem Maschinen- und Anlagenbau[17] sowie Experten für Sicherheitsmerkmale [Sch-10c, Sto-10, Völ-10] erarbeitet werden. Dabei wurden die verschiedenen Sichtweisen der beiden Positionen[18] berücksichtigt, welche Inhalte der Bereiche Sicherheitsmerkmal, Prüfung des Merkmals und Sicherheit abdecken. Die gefundenen Kriterien lassen sich passend ordnen und zu der Übersicht in Abbildung 7-3 konsolidieren. Die detaillierte Beschreibung der Kriterien ist umfangreich und befindet sich in Anhang C. Im Hauptteil hingegen wird im Folgenden die Anwendung dieser Kriterien dargestellt.

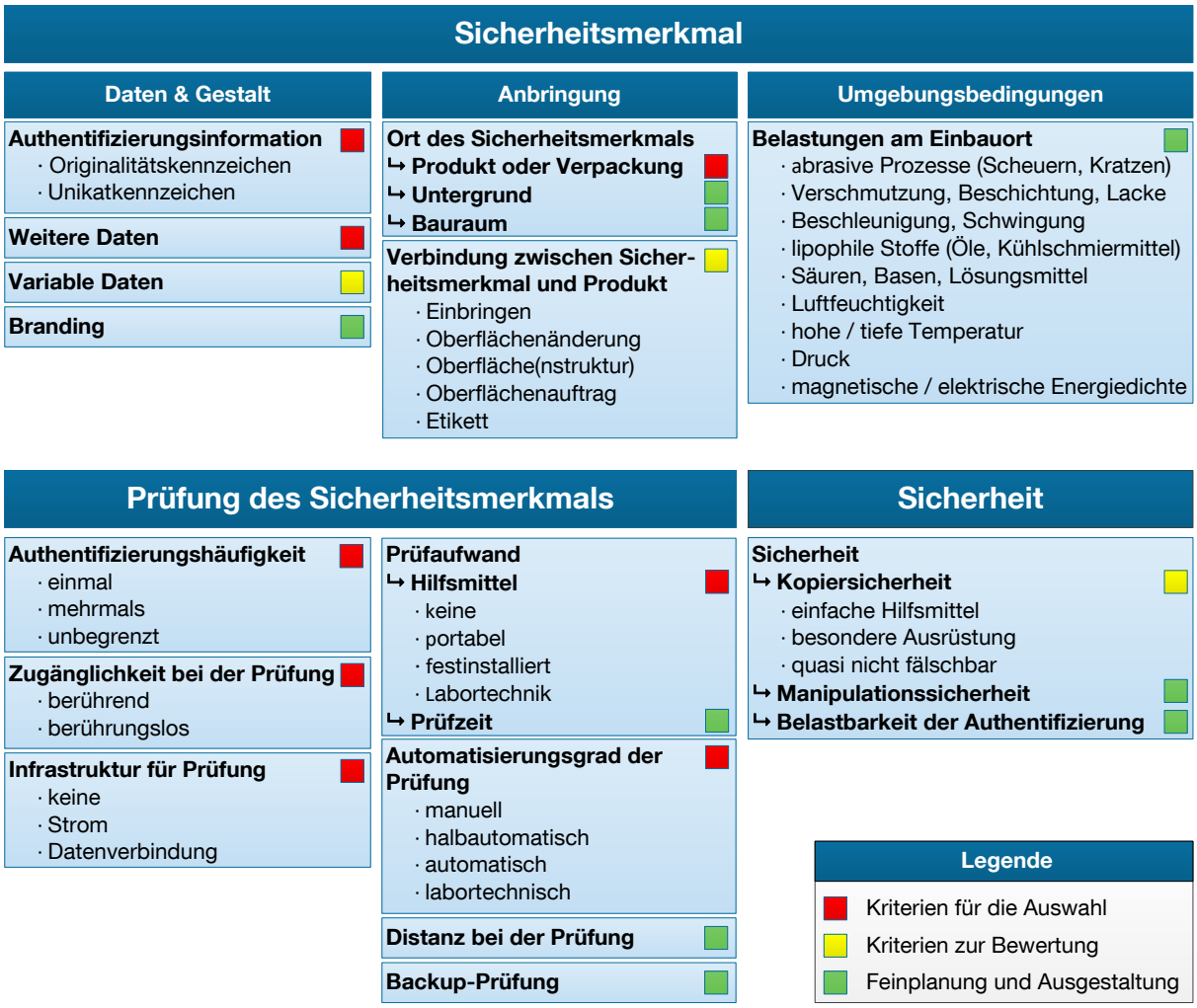


Abbildung 7-3: Strukturierte Liste technischer Auswahlkriterien

[17] Homag Group AG, Multivac Sepp Haggenmüller GmbH & Co. KG und Vollmer Werke Maschinenfabrik GmbH

[18] Anforderungen des Bauteils, Eigenschaften der Sicherheitsmerkmale

Um die in Abbildung 7-3 genannten und in Anhang C beschriebenen technischen Auswahlkriterien gemäß der in Abbildung 7-2 dargestellten Schlüssel-Schloss-Beziehung zum Einsatz zu bringen, ist es erforderlich, dass passend zu den technischen Auswahlkriterien

- die technischen Anforderungen des jeweiligen schützwenswerten Bauteils und
- die technischen Eigenschaften der Sicherheitsmerkmale

erfasst und einander gegenüber gestellt werden. So lassen sich aufgrund der technischen Anforderungen die passenden Sicherheitsmerkmale auf einfache Weise herausfiltern.

Um die Voraussetzungen dafür zu schaffen, wurden die technischen Eigenschaften der Sicherheitsmerkmale recherchiert und in einer Gesamttabelle zusammengefasst. Diese Eigenschaften wurden in Kooperation mit den Experten der Schreiner Group GmbH & Co. KG erarbeitet [Sch-10c, Sto-10, Völ-10], entstammen aus Literaturquellen oder wurden logisch ergänzt. Das Ergebnis ist eine umfangreiche Tabelle mit allen Sicherheitsmerkmalen aus Anhang A und allen Eigenschaften entsprechend der technischen Auswahlkriterien aus Abbildung 7-3, welche der Auswahl geeigneter Sicherheitsmerkmale (■) bzw. der Bewertung (■) dienen. Die Auswahlkriterien, die rein für Vorbereitungen für die Feinplanung und Ausgestaltung erforderlich sind, wurden in dieser Tabelle nicht abgebildet. Die Gesamttabelle ist in Anhang D zu finden.

Die Technologien werden permanent weiterentwickelt, so dass es sich um den zum Recherchezeitpunkt aktuellen Stand handelt, der sich mit der Zeit verändern wird. Im Fokus steht die Methode der Auswahl der je schützenswertem Bauteil passenden Sicherheitsmerkmale, die mit dieser Gesamtübersicht sehr gut darstellbar und nachvollziehbar ist.

7.1.2 Vorgehen zur Bestimmung der passenden Sicherheitsmerkmale auf Basis der technischen Auswahlkriterien

Zur Relevanz der einzelnen Kriterien wurde eine umfangreiche Analyse auf Basis von 31 Technologien und 22 Bauteilen mit den in Abbildung 7-3 gelisteten 15 Kriterien und acht Unterkriterien durchgeführt. Dabei hat sich gezeigt, dass diese Kriterien sinnvoll in einem stufenweisen Vorgehen zur Bestimmung der passenden Sicher-

heitsmerkmale eingesetzt werden können (die farbliche Markierung ist identisch mit Abbildung 7-3):

1. Kriterien für die Auswahl geeigneter Sicherheitsmerkmale:
   Die Ausprägungen dieser Kriterien, die durch das jeweils betrachtete schützenswerte Bauteil vorgegeben sind, müssen seitens der Sicherheitsmerkmale erfüllbar sein.
2. Kriterien zur Bewertung:
   Die Ausprägungen dieser Kriterien werden bei der Suche innerhalb der geeigneten Sicherheitsmerkmale in bewertender Weise berücksichtigt. Diese Kriterien haben nur geringen Einfluss auf die Auswahl der Sicherheitsmerkmale, da Voraussetzungen für die Erfüllung dieser Kriterien bereits in Kriterien aus Punkt 1 abgebildet sind. Im Falle der „Kopiersicherheit“ soll zudem der Fokus nicht zu früh zu eng werden und alle noch zur Verfügung stehenden Sicherheitsmerkmale für den Anwender noch sichtbar sein. Zumal auch mit einer Kombination von Sicherheitsmerkmalen das gewünscht Sicherheitsniveau erreicht werden kann.
3. Vorbereitungen für die Feinplanung und Ausgestaltung:
   Die Ausprägungen dieser Kriterien werden lediglich bei der Ausgestaltung des Sicherheitsmerkmals für die Implementierung genutzt, da sich in der Praxis gezeigt hat, dass die Sicherheitsmerkmale sehr gut an die Anforderungen, die aus diesen Kriterien entstehen, angepasst werden können.

Die Verwendung der Kriterien wird in den nächsten Abschnitten jeweils mit Hinweisen zur Auswahl der passenden Ausprägungen dargestellt.

7.1.2.1 Kriterien für die Auswahl geeigneter Sicherheitsmerkmale ( )

Wie Abbildung 7-3 entnommen werden kann, müssen für die Auswahl geeigneter Sicherheitsmerkmale die rot markierten technischen Auswahlkriterien berücksichtigt werden. Diese werden hier in einer bezüglich der Bearbeitung sinnvollen Reihenfolge mit Hinweisen zur Auswahl der passenden Ausprägungen dargestellt und bezüglich des beschriebenen Anwendungsfalls im Maschinen- und Anlagenbau erläutert.

Ort des Sicherheitsmerkmals (Produkt oder Verpackung)

Für den Ort des Sicherheitsmerkmals (Beschreibung siehe Anhang C.5.1) kommt lediglich die Ausprägung „Produkt“ in Frage, da Komponenten und Ersatzteile wäh-

rend der gesamten Lebensdauer als Originale erkannt werden sollen (siehe Abschnitte 1.2.2, S. 8 und 5.4, S. 95). Eine Kennzeichnung der Verpackung wäre lediglich eine zusätzliche Möglichkeit. Sollte dies gewünscht werden, kann diese Auswahlmethode prinzipiell auch für Verpackungen durchlaufen werden.

Authentifizierungshäufigkeit

Bei der Authentifizierungshäufigkeit ist für schützenswerte Bauteile in Maschinen oder Anlagen die Ausprägung „unbegrenzt“ sinnvoll – ansonsten könnte es passieren, dass die Originalität eines Bauteils während der Lebensdauer gar nicht mehr geprüft oder nachgewiesen werden kann. Dies ist jedoch eine zentrale Anforderung an das Sicherheitsmerkmal (siehe Abschnitt 5.4.1, S. 96).

Authentifizierungsinformation

Eine zentrale Frage bei der Auswahl von Sicherheitsmerkmalen bezieht sich auf die Authentifizierungsinformation (Beschreibung siehe Anhang C.1) und somit die Frage, ob ein „Originalitätskennzeichen“ ausreicht oder ein „Unikatkennzeichen“ eingesetzt werden soll. Diese Ausprägung hat weitreichende Konsequenzen. Wird ein Unikatkennzeichen gewählt, ist bei der Gestaltung eines Systems zur Authentifizierung schützenswerter Bauteile mittels Sicherheitsmerkmalen ein teilebezogenes T&T möglich. Mit einem Originalitätskennzeichen kann der Weg eines individuellen Produkts im Wertschöpfungsnetzwerk nicht verfolgt und dokumentiert werden. Auch hat diese Auswahl Auswirkungen auf die Sicherheit im System. Sollte es einem unredlichen Wettbewerber gelingen, ein Unikatkennzeichen zu kopieren, so kann dieser nur dieses eine Unikat imitieren, was bei einer Plausibilitätsprüfung von T&T-Daten zutage tritt. Denn ein als Unikat gekennzeichnetes Produkt kann sich nicht an verschiedenen Orten oder in verschiedenen Maschinen gleichzeitig befinden. Diese Plausibilitätsprüfung ist bei Originalitätskennzeichen nicht möglich. Ein häufig gewählter Weg ist jedoch die Kombination eines passenden Originalitätskennzeichens mit einem Identitätskennzeichen (siehe Abschnitt 7.3).

Weitere Daten

Die Entscheidung für weitere Daten (Beschreibung siehe Anhang C.2), die neben der Authentifizierungsinformation im Sicherheitsmerkmal selbst enthalten sein sollen, schränkt die Menge passender Merkmale weiter ein. Zunächst ist dafür Vorausset-

zung, dass ein Unikatkennzeichen gewählt wurde[19]. Jedoch ist es nicht bei jedem Unikatkennzeichen möglich, weitere Daten zu integrieren. Ein Beispiel dafür ist die Oberflächenauthentifizierung (siehe Anhang A.5.5.3).

Zugänglichkeit bei der Prüfung

Wenn eine automatische Authentifizierung von Bauteilen im verbauten Zustand in Maschinen und Anlagen angestrebt wird, ist es aus Gründen der Praktikabilität bezüglich der Zugänglichkeit bei der Prüfung (Beschreibung siehe Anhang C.9) sinnvoll, ein Sicherheitsmerkmal zu wählen, das berührungslos arbeitet.

Infrastruktur für Prüfung

Die verbleibenden drei Auswahlkriterien zur Bestimmung geeigneter Sicherheitsmerkmale „Infrastruktur für Prüfung“, „Prüfaufwand (Hilfsmittel)“ und „Automatisierungsgrad der Prüfung“ hängen stark miteinander zusammen. Die bei diesen drei Kriterien gewählten Ausprägungen bedingen sich gegenseitig[20] und beeinflussen das innerhalb des Systems erreichbare Sicherheitsniveau (siehe Abbildung 7-4).

Bei der Bestimmung der vorhandenen Infrastruktur für die Prüfung (Beschreibung siehe Anhang C.10) muss festgestellt werden, welche Infrastruktur am Prüfort vorhanden ist. Der Ort, an dem die Prüfung stattfindet, kann prinzipiell jeder Ort im Wertschöpfungsnetzwerk sein. Aber die Bauteile und Komponenten sollten zur vollständigen Implementierung des Systems auch bei ihrem Einsatz in Maschinen / Anlagen authentifiziert werden können. Daher ist die Feststellung der vorhandenen Medien auf den Maschinen / Anlagen besonders wichtig. Elektrischer Strom dürfte immer verfügbar sein. Datenverbindungen sind zwar häufig möglich, aber nicht immer aktiv. In dem Fall, dass keine Datenverbindung permanent verfügbar ist, sollte ein Sicherheitsmerkmal gewählt werden, das auch ohne Datenverbindung authentifiziert werden kann.

[19] bis auf eine Ausnahme, siehe Anhang A.5.4.10 bzw. Tabelle D.1

[20] beispielsweise wäre eine automatisierte Prüfung ohne Strom nicht möglich

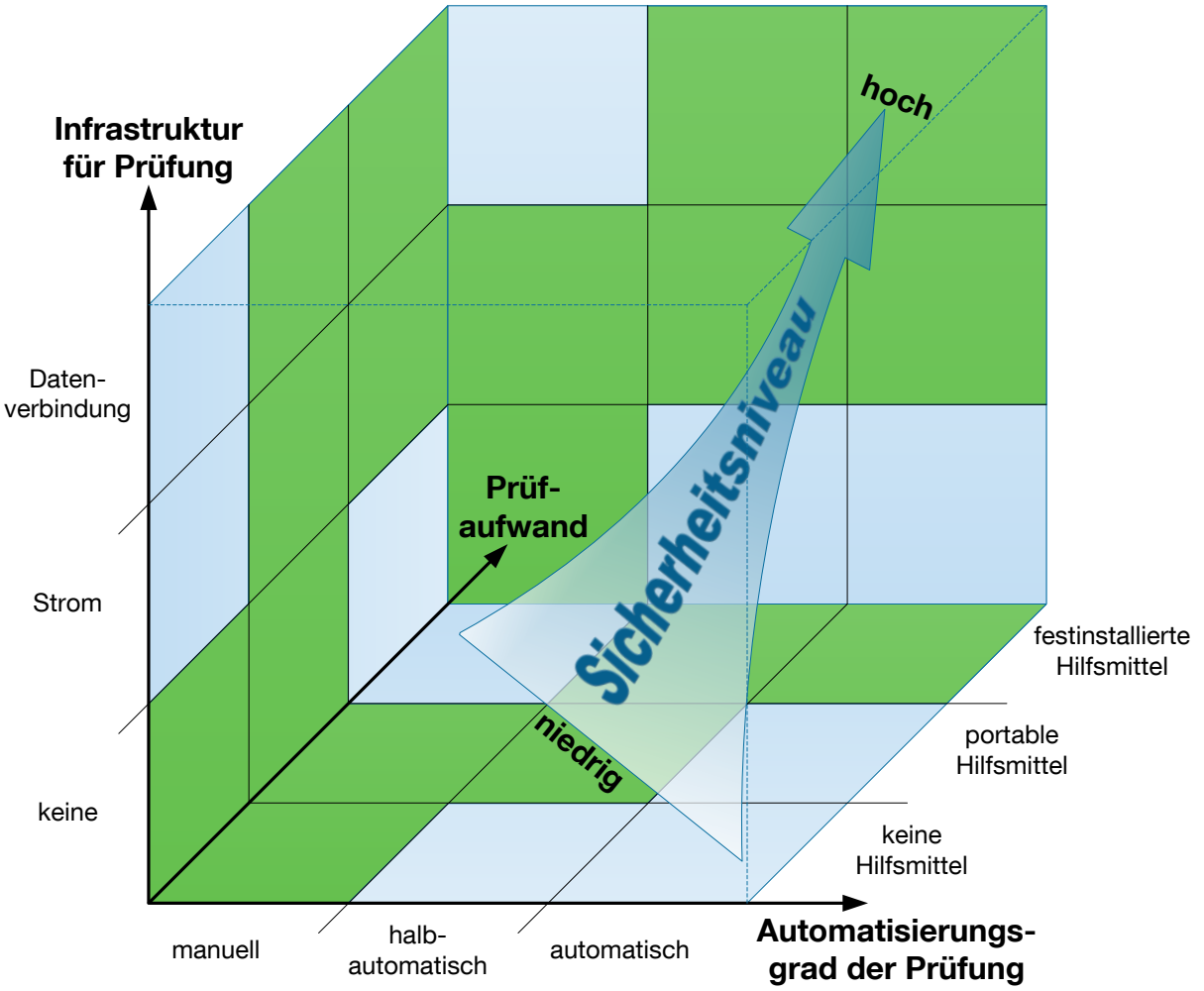


Abbildung 7-4: **Qualitativer Zusammenhang zwischen den technischen Auswahlkriterien „Infrastruktur für Prüfung“, „Prüfaufwand (Hilfsmittel)“, „Automatisierungsgrad der Prüfung“ und dem erreichbaren Sicherheitsniveau (grün markierte Felder erschließen mögliche Kombinationen)**

Prüfaufwand (Hilfsmittel)

Die Hilfsmittel, welche bei der Authentifizierung eingesetzt werden sollen (Beschreibung siehe Anhang C.11.1), bestimmen einerseits maßgeblich den zeitlichen wie auch monetären Prüfaufwand und andererseits das erreichbare Sicherheitsniveau. Zudem ist deren Auswahl stark abhängig von der vorhandenen Infrastruktur[21].

Bei rein manuellen Authentifizierungen ohne Hilfsmittel ist die Feststellung der Originalität nur durch den jeweils geschulten Mitarbeiter möglich. Wenn dessen Prüfung durch entsprechende portable Hilfsmittel unterstützt wird, ist der Authentifizierungs-

[21] sollte beispielsweise kein Strom vorhanden sein können auch keine festinstallierten Hilfsmittel betrieben werden

schritt stärker abgesichert – insbesondere, wenn es sich um elektronische Hilfsmittel handelt.

Bei festinstallierten Hilfsmitteln gibt es zwei Vorteile: Entweder kann der Bediener durch entsprechende Steuerungen unterstützt werden, so dass die Authentifizierungen gemäß einer Vorgabe beispielsweise regelmäßig stattfindet, oder es können auch Technologien genutzt werden, deren Prüfung größere Prüfgeräte bedingen.

Labortechnik sollte im Bereich des Maschinen- und Anlagenbaus nicht gewählt werden, da das Prüfergebnis dann nicht unmittelbar verfügbar wäre und somit der präventive Charakter der Maßnahme verloren ginge. Auch wäre der Prüfaufwand sehr groß. Daher ist Labortechnik in Abbildung 7-4 nicht berücksichtigt.

Automatisierungsgrad der Prüfung

Bei der Bestimmung des gewünschten Automatisierungsgrades der Prüfung (Beschreibung siehe Anhang C.12) hat die Wahl einer automatischen Prüfung Vorteile.

Bei einer automatischen Prüfung können Fehler, die bei einer manuellen Prüfung entstehen können, weitestgehend ausgeschlossen werden. Zunächst findet die Authentifizierung gemäß einem beispielsweise in einer Steuerung vorher festgelegten Ablauf statt und ein „Vergessen“ ist somit ausgeschlossen. Auch bezüglich der Zuverlässigkeit des Prüfergebnisses hat eine automatische Prüfung große Vorteile. Sofern das Sicherheitsmerkmal nicht beschädigt ist, ist das Prüfergebnis höchst zuverlässig.

Bei einer halbautomatischen Prüfung mit beispielsweise einem an der Maschine oder Anlage angebundenen Handscanner kann auch davon ausgegangen werden, dass das Prüfergebnis äußerst zuverlässig ist. Dies stellt somit auch eine sehr gute Wahl dar, zumal nicht alle Prüfungen technologiebedingt völlig automatisierbar sind.

Eine rein manuelle Prüfung birgt immer Fehlerpotenzial und die Prüfergebnisse sind daher weniger belastbar.

Wie im Kriterium zuvor „Prüfaufwand (Hilfsmittel)“ dargestellt, sollte eine rein labortechnische Prüfung im Maschinen- und Anlagenbau nicht eingesetzt werden.

Ergebnis

Aufgrund der Festlegung der Ausprägungen für die Kriterien, die sich aufgrund der Anforderungen an ein Sicherheitsmerkmal durch das betrachtete schützenswerte

Bauteil ergeben, ist es innerhalb dieses Abschnitts möglich, die Menge aller in Tabelle D-1 im Anhang D gelisteten Sicherheitsmerkmale auf die Menge der geeigneten Sicherheitsmerkmale einzuschränken. Dies basiert auf dem in Abbildung 7-2 dargestellten Schlüssel-Schloss-Prinzip.

7.1.2.2 Kriterien zur Bewertung ( )

Nach der Anwendung der „Kriterien zur Auswahl“ (siehe Abschnitt 7.1.2.1) sind in der verbleibenden Menge an geeigneten Sicherheitsmerkmalen die Anforderungen, welche aus Sicht des schützenswerten Bauteils an das Sicherheitsmerkmal gestellt werden, bereits abgebildet. In diesem Abschnitt werden die verbleibenden Sicherheitsmerkmale mit Hilfe der in Abbildung 7-3 gelb markierten Bewertungskriterien priorisiert.

Variable Daten

Ob auf einem Sicherheitsmerkmal neben der Authentifizierungsinformation und etwaigen weiteren Daten zudem auch variable Daten (Beschreibung siehe Anhang C.3) sinnvoll sind, hängt einerseits vom geplanten Weg des Produkts durch die Wertschöpfungskette und andererseits von der Ausgestaltung des gesamten Systems zur Kennzeichnung und Authentifizierung der schützenswerten Bauteile ab. Variable Daten sind, wie dies in Tabelle D-1 im Anhang D entnommen werden kann, lediglich bei einem kontaktbehafteten Mikrochip (siehe Anhang A.3.5) oder bei RFID (siehe Anhang A.3.6) möglich. Im Sicherheitsmerkmal variabel zu speichernde Daten können beispielsweise sein:

- T&T-Informationen: produktbezogene Historie des Bauteils über den Weg im Wertschöpfungs- und Logsitiknetzwerk
- produktbezogene Sensorinformationen wie Temperaturen, Lichteinfall u. Ä. aufgrund Sensorerfassung in der Umgebung oder am Produkt selbst
- prozessbezogene Sensorinformationen wie Drehmomentangaben bei Montageschritten u. Ä.
- Hinweise für die weiteren Be- / Verarbeitungs- / Montageschritte
- Baugruppen-/ Rüstsatzinformationen mit zusammengehörenden Bauteilen
- Mitarbeiter- oder Bearbeiterinformationen bei beispielsweise Inline-Qualitätssicherungsmaßnahmen

In der Praxis hat sich herausgestellt, dass variable Daten auf den Produkten deshalb meist nicht notwendig sind, weil diese Daten auch in einem entsprechenden IT-System mit Datenbanken (siehe Abschnitt 8.3, S. 188) abgelegt werden können. Die Verknüpfung dieser Daten mit den Produkten erfolgt über Unikatkennzeichen an den Produkten.

Verbindung zwischen Sicherheitsmerkmal und Produkt

Dieses Kriterium ist in Anhang C.6 mit fünf möglichen Ausprägungen beschrieben. Das Einbringen eines Sicherheitsmerkmals ist eine sehr sichere Möglichkeit der physischen Verbindung zwischen Sicherheitsmerkmal und Produkt (siehe Abbildung 7-5). Das Sicherheitsmerkmal wird dabei in das Substrat des Produktes gelegt oder gemischt und ist somit nach dem Herstellprozess in einer gewissen Konzentration im gesamten Produkt vorhanden. Dies ist beispielsweise bei Partikeln mit Röntgenlumineszenz- oder mit UV-Eigenschaften, mit Mikropunkten oder Nanopartikeln möglich (siehe Anhang A.5.4.3.2, A.5.4.3.4, A.5.4.10 und A.6.3).

Bei Nutzung der Oberfläche(nstruktur) oder bei der gezielten Erzeugung einer besonderen Oberfläche wird mit Verfahren der Oberflächenauthentifizierung gearbeitet (siehe Anhang A.5.5.3).

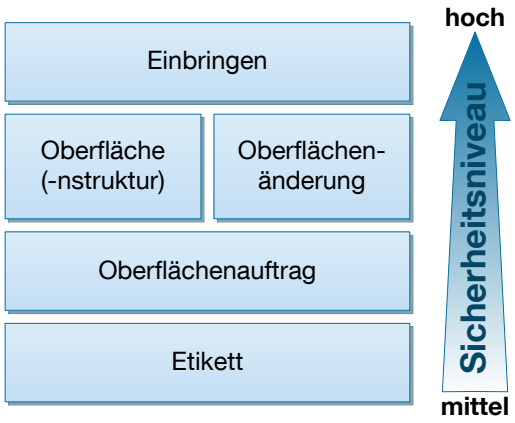


Abbildung 7-5: Qualitative Einordnung der Verbindungen zwischen Sicherheitsmerkmal und Produkt und dem erreichbaren Sicherheitsniveau

Das Aufbringen eines Sicherheitsmerkmals durch einen Oberflächenauftrag ist mit vielen besonderen Farben und Partikeln möglich und stellt eine sehr gute Form der Direktmarkierung von Produkten dar. Dies kann durch die Kennzeichnung an einer oder mehreren Stellen am Bauteil erfolgen, oder massenhaft, wie dies bei den Mikropunkten erfolgt, die mit Aerosolspray aufgetragen werden (siehe Anhang A.5.4.10).

Eine sehr beliebte Methode ist das Aufbringen des Sicherheitsmerkmals in Form eines Etiketts. Das entspricht zwar meist der Anforderung der Wirtschaftlichkeit, häufig jedoch nicht immer der Forderung nach Dauerhaftigkeit des Sicherheitsmerkmals (siehe Abschnitt 5.4.1, S. 96). Denn ein Etikett kann beschädigt werden, verloren gehen oder schlimmstenfalls absichtlich vom Originalprodukt auf eine Kopie übertragen werden. Das Problem liegt dabei in der physischen Verbindung zwischen Etikett und Produkt. Es gibt jedoch Möglichkeiten, sehr haltbare und dauerhafte Verbindungen herzustellen, sowie Manipulationsversuche anzuzeigen, um den Versuch der Übertragung des Etiketts auf ein kopiertes Bauteil zu verhindern. Diese Gestaltung des Sicherheitsmerkmals muss im Einzelfall von Experten vorgenommen werden. Der Vorteil von Etiketten liegt darin, dass auf einem Etikett sehr einfach mehrere verschiedene Sicherheitsmerkmale integriert werden können, um das Sicherheitsniveau der Lösung weiter anzuheben [Sch-13b, Sch-13c, Sch-13d]. So entsteht auch die Vielzahl an kombinierten Sicherheitsprodukten, die diverse Firmen am Markt anbieten.

Eine hochinteressante Möglichkeit der Verbindung zwischen Originalbauteil und Sicherheitsmerkmal stellen nicht identisch reproduzierbare Funktionen dar, sogenannte POWFs (Physical One-Way Function). Nach Definition von *Ravikanth* sind POWFs wie folgt definiert:

Physical One-Way Function (POWF):
POWFs sind Wechselwirkungen zwischen einem physikalischen System und einem Gegenstand, wobei das System sich in einem undefinierten internen Zustand befindet. Ergebnis sind physikalisch schwer oder sogar nicht reproduzierbare produktbezogene Eigenschaften wie absolute Endmaße, gemessene Oberflächenstruktur, absolutes Gewicht u. Ä. [Rav-01 S. 16]

Bei der Übertragung dieser Definition in produktionstechnische Abläufe kann festgestellt werden, dass viele hergestellte Strukturen deshalb einmalig sind, weil der Herstellprozess eine POWF darstellt: Papierproduktion, Herstellung von Holzpressspan-Produkten, fräsende Bearbeitung einer Metalloberfläche, Härteprozesse, Wafer-Produktion u. v. m. Diese Strukturen werden beispielsweise bei der Oberflächenauthentifizierung (siehe Anhang A.5.5.3) genutzt, können aber auch in digitalisierter Form, z. B. als hochauflösendes Bild, im Sicherheitsmerkmal als variable Daten abgelegt werden.

Diese Möglichkeit ist deshalb hochinteressant, weil die Überprüfung des Sicherheitsmerkmals und der variablen Daten, also auch der POWF, eine sichere Methode darstellt, um Originale zu authentifizieren und auch sehr gute Kopien zu entdecken. Dies liegt an der Nicht-Reproduzierbarkeit der POWFs. Gleichzeitig erzeugt diese Kombination eine einmalige Verbindung zwischen Sicherheitsmerkmal und Produkt. Ein Übertragen des Sicherheitsmerkmals auf ein kopiertes Bauteil ist zwar denkbar, wird aber bei der nächsten Überprüfung sofort erkannt.

Sicherheit (Kopiersicherheit)

Zur Bewertung der Kopiersicherheit (Beschreibung siehe Anhang C.15.1) sind für die gelisteten Sicherheitsmerkmale in Tabelle D-1 im Anhang D Einstufungen angegeben, mittels derer festgestellt werden kann, wie sicher die Merkmale gegen Kopieren sind, nämlich

- reichen „einfache Hilfsmittel“, um eine Kopie des Sicherheitsmerkmals herzustellen, oder
- ist eine „besondere Ausrüstung“ notwendig, oder
- ist das Sicherheitsmerkmal „quasi nicht fälschbar“.

Ergebnis

Die Ergebnisse aus den drei Bewertungskriterien „Variable Daten“, „Verbindung zwischen Sicherheitsmerkmal und Produkt“ und „Sicherheit (Kopiersicherheit)“ ergibt eine Einstufung der nach dem ersten Abschnitt verbleibenden geeigneten Sicherheitsmerkmale (siehe Abschnitt 7.1.2.1) und ermöglicht eine klare Priorisierung.

7.1.2.3 Vorbereitungen für Feinplanung und Ausgestaltung (■)

Nach der Bestimmung der für ein schützenswertes Bauteil prinzipiell geeigneten Sicherheitsmerkmale in Abschnitt 7.1.2.1 und nach deren priorisierender Bewertung in Abschnitt 7.1.2.2 erfolgen in diesem Abschnitt die Vorbereitungen für die Feinplanung und Ausgestaltung. Im Folgenden sind die in Abbildung 7-3 grün markierten Kriterien in einer bezüglich der Bearbeitung sinnvollen Reihenfolge aufgenommen und jeweils mit Hinweisen zur Auswahl der passenden Ausprägungen dargestellt.

Ort des Sicherheitsmerkmals (Untergrund, Bauraum)

Beim Ort des Sicherheitsmerkmals ist noch die Frage nach dem Untergrund und dem verfügbaren Bauraum offen (Beschreibungen siehe Anhang C.5.2 und C.5.3).

Der verfügbare Bauraum kann die Größe des einsetzbaren Sicherheitsmerkmals begrenzen, der Untergrund kann bestimmte Verbindungstechniken zwischen Sicherheitsmerkmal und schützenswertem Bauteil erforderlich machen. In der Praxis hat sich gezeigt, dass beide Anforderungen zwar wichtig sind, aber in der Feinplanung und Ausgestaltung des Sicherheitsmerkmals durch eine spezifische Anpassung abgebildet werden können und damit die Technologieentscheidung nicht beeinflussen.

Belastungen am Einbauort

Die Belastungen am Einbauort, die auf ein schützenswertes Bauteil wirken und somit auch auf das Sicherheitsmerkmal, können sehr vielfältiger Natur sein (Beschreibung siehe Anhang C.7). Dabei können auch Belastungen auf das Sicherheitsmerkmal einwirken, welche das Merkmal zerstören. Da dies jedoch sehr selten ist und zudem häufig durch entsprechende Platzierung und Ausgestaltung des Sicherheitsmekmals verhindert werden kann, wurde dieses Kriterium in diesen Abschnitt übernommen.

Distanz bei der Prüfung

Die notwendige oder minimal mögliche Distanz bei der Prüfung (Beschreibung siehe Anhang C.13) ist bereits teilweise im Kriterium „Zugänglichkeit bei der Prüfung“ berücksichtigt. Die räumlichen Gegebenheiten am Einbauort des schützenswerten Bauteils in der Maschine oder Anlage sollten für die Gestaltung des Prüfvorgangs genau untersucht werden. Dabei ist die minimal einzuhaltende Distanz bei der Prüfung von Interesse, da dies Auswirkungen auf etwaige einzusetzende Hilfsmittel haben kann. Da dies in der Praxis meist lediglich Auswirkungen auf die technische Ausstattung eines etwaigen eingesetzten Prüfhilfsmittels hat, ist es ausreichend, diese Frage in Vorbereitung auf die Feinplanung und Ausgestaltung zu beantworten.

Prüfaufwand (Prüfzeit)

Die Prüfzeit (Beschreibung siehe Anhang C.11.2) ist stark von den bereits gewählten Hilfsmitteln für die Prüfung abhängig, kann jedoch nach Festlegung des Hilfsmittels in gewissen Grenzen beeinflusst werden und wird daher in diesem Abschnitt mit aufgenommen.

Sicherheit (Manipulationssicherheit, Belastbarkeit der Authentifizierung)

Bezüglich der Sicherheit wurde bei den Bewertungskriterien in Abschnitt 7.1.2.2 bereits die Frage nach der Kopiersicherheit des Sicherheitsmerkmals berücksichtigt. Die Aspekte Manipulationssicherheit und Belastbarkeit der Authentifizierung sind

stark von der Feinplanung des Sicherheitsmerkmals sowie der Ausgestaltung des Prozesses bei der Aufbringung des Merkmals abhängig (Beschreibung siehe Anhang C.15.2 und C.15.3).

Die Manipulationssicherheit eines Sicherheitsmerkmals ist von der konkreten Ausgestaltung der Verbindung zwischen Kennzeichen und Produkt abhängig. Diese Verbindung kann durch entsprechende Maßnahmen manipulationssicher gegen z. B. eine Übertragung auf eine andere Ware gestaltet werden, ist aber vom konkreten Anwendungsfall abhängig und ist in der Feinplanung mit Unterstützung durch Fachexperten erreichbar.

Die Belastbarkeit der Authentifizierung hängt stark mit der Ausgestaltung der Prozesse bei der Herstellung und Markierung der Originalwaren zusammen. Durch passende Maßnahmen im Prozess muss nachweisbar sichergestellt sein, dass jedes Originalprodukt, welches verkauft wird, ein Sicherheitsmerkmal trägt. Zudem dürfen keine Blanko-Sicherheitsmerkmale das Unternehmen verlassen[22]. So ist sichergestellt, dass das ein- oder aufgebrachte Sicherheitsmerkmal auch im Extremfall bei gerichtlichen Auseinandersetzungen Bestand hat.

Branding

Das Branding der Originalbauteile wurde bereits in Kapitel „6 Branding: Kennzeichnung schützenswerter Komponenten und Ersatzteile mit unternehmenseigenen Marken“, S. 101 als Kennzeichnung mit eingetragenen Markenzeichen beschrieben. Zusätzlich ist das Element als technisches Kriterium für diesen Abschnitt der Vorbereitungen für die Feinplanung und Ausgestaltung angeführt, weil auch innerhalb des Sicherheitsmerkmals Marken Verwendung finden können (Beschreibung siehe Anhang C.4). So entsteht ein doppelter Schutz: Der Schutz durch das Sicherheitsmerkmal selbst sowie ein rechtlicher Schutz aufgrund der Rechte für das eingetragene Markenzeichen. Beispielsweise können Markenzeichen sehr gut in Hologramme integriert werden (siehe Abbildung 7-6).

[22] Dass das Sicherheitsmerkmal nicht zufällig zweimal existiert, ist ebenso eine Voraussetzung (siehe Abschnitt 5.4.1, S. 91).

Abbildung 7-6: **Integration eines eingetragenen Markenzeichens in ein Sicherheitsmerkmal am Beispiel von Hologrammen: Drahttransportrolle der Firma Vollmer Werke Maschinenfabrik GmbH (links) und Handy-Akku der Nokia GmbH (Bildquelle Bauteil: Vollmer Werke Maschinenfabrik GmbH, Bildquellen Akku: [Chi-04, Nok-09 S. 12])**

Backup-Prüfung

Das letzte Kriterium, das betrachtet werden sollte, ist die Frage nach einer Backup-Prüfung (Beschreibung siehe Anhang C.14). Die Backup-Prüfung ist ein zweiter Weg der Authentifizierung eines Originalprodukts für den Fall, dass das Haupt-Sicherheitsmerkmal ausfällt und das Produkt weiterhin als Original authentifiziert werden muss. Im Falle, dass dies für das jeweilige schützenswerte Bauteil wichtig und notwendig ist, kann die hier vorgestellte Methode zur Auswahl eines Sicherheitsmerkmals erneut durchlaufen werden mit dem Ziel, ein weiteres Sicherheitsmerkmal zu bestimmen.

7.1.3 Beispiele zur Bestimmung der je schützenswertem Bauteil passenden Sicherheitsmerkmale auf Basis technischer Auswahlkriterien

In Abschnitt 5.2.2, S. 89 wurden auf Basis der allgemeingültig formulierten Auswahlkriterien für schützenswerte Bauteile beispielhaft die in Abbildung 5-4, S. 90 dargestellten Bauteile bestimmt. Aus diesen sieben Bauteilen werden hier fünf schützenswerte Bauteile ausgewählt, die als durchgängiges Beispiel auch in den folgenden Kapiteln dienen sollen. An diesen ausgewählten schützenswerten Bauteilen wird das Vorgehen zur Bestimmung passender Sicherheitsmerkmale auf Basis technischer Auswahlkriterien gezeigt:

- Firma Homag: Aggregate / HSK-Schnittstelle
- Firma Multivac: Klammerkette
- Firma Multivac: Siegeldichtung
- Firma Vollmer: Einmesslehre
- Firma Vollmer: Drahttransportrolle

Die Anzahl der Beispiele scheint recht groß, ist aber sinnvoll, weil in Kapitel 8 dargestellt werden soll, wie verschiedene Authentifizierungstechnologien bei verschiedenen Teilnehmern in ein technisches Gesamtsystem integriert werden können.

7.1.3.1 Angaben der Unternehmen bezüglich der technischen Auswahlkriterien

Die Beispielunternehmen aus dem Maschinen- und Anlagenbau haben zu ihren schützenswerten Bauteilen entsprechende Angaben gemacht. Diese Angaben wurden für alle Kriterien, die später zur Auswahl, Bewertung und Ausgestaltung der Sicherheitsmerkmale benötigt wurden, eingeholt. Die Ergebnisse sind in Tabelle 7-1, Tabelle 7-2, Tabelle 7-3, Tabelle 7-4 und Tabelle 7-5 abgebildet. Mit Hilfe dieser Angaben wurde der Auswahlprozess, wie in Abschnitt 7.1.2 dargestellt, durchlaufen.

Tabelle 7-1: Angaben der HOMAG Holzbearbeitungssysteme GmbH für die Aggregate / HSK-Schnittstelle bzgl. der Auswahlkriterien

	HOMAG Holzbearbeitungssysteme GmbH: Aggregate / HSK-Schnittstelle	
	Kriterium	**angegebene Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	Produkt
	Authentifizierungshäufigkeit	unbegrenzt
	Authentifizierungsinformation	Unikatkennzeichen
	Weitere Daten	nein (inkludiert ebenfalls Technologien, bei denen ein "ja" angegeben ist)
	Zugänglichkeit bei der Prüfung	berührend (diese Angabe impliziert, dass „berührungslos“ auch möglich ist)
	Infrastruktur für Prüfung	offline, d.h. Strom vorhanden, „keine“ ebenfalls möglich
	Prüfaufwand (Hilfsmittel)	portabel oder festinstalliert
	Automatisierungsgrad der Prüfung	halbautomatisch für Service, automatisch an der Maschine
Kriterien zur Bewertung	Variable Daten	nein (inkludiert ebenfalls Technologien, bei denen ein "ja" angegeben ist)
	Verbindung zwischen Sicherheitsmerkmal und Produkt	alle Verbindungsmöglichkeiten außer „einbringen“
	Sicherheit (Kopiersicherheit)	besondere Ausrüstung (diese Angabe impliziert, dass "quasi nicht fälschbar" auch möglich ist)
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	metallisch, i. d. R. Werkzeugstahl
	Ort des Sicherheitsmerkmals (Bauraum)	voluminöse Markierung möglich
	Belastungen am Einbauort	Verschmutzungen durch Holzspäne und -staub, Maximaltemperatur 80 °C
	Distanz bei der Prüfung	> 0 mm möglich, situations- & konstruktionsabhängig
	Prüfaufwand (Prüfzeit)	< 60 s bei halbautomatischer / automatischer Prüfung
	Sicherheit (Manipulationssicherheit)	wenigstens sollte für einen Manipulationsversuch Spezialausrüstung notwendig sein
	Sicherheit (Belastbarkeit der Authentifizierung)	Das System sollte einen Mehrwert für Kunden, interne Überprüfungen der Originalität sowie einen gerichtsverwertbaren Nachweis der Originalität ermöglichen.
	Branding	gerne, falls möglich
	Backup-Prüfung	keine

Tabelle 7-2: Angaben der Multivac Sepp Haggenmüller GmbH & Co. KG für die Klammerkette bzgl. der Auswahlkriterien

	Multivac Sepp Haggenmüller GmbH & Co. KG: Klammerkette	
	Kriterium	**angegebene Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	Produkt
	Authentifizierungshäufigkeit	unbegrenzt
	Authentifizierungsinformation	Unikatkennzeichen
	Weitere Daten	ja
	Zugänglichkeit bei der Prüfung	berührungslos
	Infrastruktur für Prüfung	offline, d.h. Strom vorhanden, „keine“ ebenfalls möglich
	Prüfaufwand (Hilfsmittel)	festinstalliert
	Automatisierungsgrad der Prüfung	automatisch an der Maschine
Kriterien zur Bewertung	Variable Daten	ja
	Verbindung zwischen Sicherheitsmerkmal und Produkt	alle Verbindungsmöglichkeiten außer „einbringen“
	Sicherheit (Kopiersicherheit)	besondere Ausrüstung (diese Angabe impliziert, dass "quasi nicht fälschbar" auch möglich ist)
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	metallisch, i. d. R. Stahl
	Ort des Sicherheitsmerkmals (Bauraum)	sehr begrenzter Bauraum, dennoch voluminöse Markierung möglich
	Belastungen am Einbauort	abrasive Prozesse, Verschmutzungen durch Verpackungsgut, Beschleunigungen und Schwingungen, lipophile Stoffe (Minimalschmierung, Verpackungsgut), starke Reinigungsmittel, hohe Luftfeuchtigkeit
	Distanz bei der Prüfung	> 0 mm möglich, situations- & konstruktionsabhängig
	Prüfaufwand (Prüfzeit)	0 s bei automatischer Prüfung, d. h. Authentifizierung im laufenden Betrieb
	Sicherheit (Manipulationssicherheit)	nicht manipulierbar, d. h. selbstzerstörend bei einem Manipulationsversuch
	Sicherheit (Belastbarkeit der Authentifizierung)	Das System sollte einen Mehrwert für Kunden, interne Überprüfungen der Originalität sowie einen gerichtsverwertbaren Nachweis der Originalität ermöglichen.
	Branding	gerne, falls möglich
	Backup-Prüfung	keine

Tabelle 7-3: Angaben der Multivac Sepp Haggenmüller GmbH & Co. KG für die Siegeldichtung bzgl. der Auswahlkriterien

	Multivac Sepp Haggenmüller GmbH & Co. KG: Siegeldichtung	
	Kriterium	**angegebene Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	Produkt
	Authentifizierungshäufigkeit	unbegrenzt
	Authentifizierungsinformation	Unikatkennzeichen
	Weitere Daten	ja
	Zugänglichkeit bei der Prüfung	berührungslos
	Infrastruktur für Prüfung	offline, d.h. Strom vorhanden, „keine“ ebenfalls möglich
	Prüfaufwand (Hilfsmittel)	festinstalliert
	Automatisierungsgrad der Prüfung	automatisch an der Maschine
Kriterien zur Bewertung	Variable Daten	ja
	Verbindung zwischen Sicherheitsmerkmal und Produkt	alle Verbindungsmöglichkeiten außer „einbringen“
	Sicherheit (Kopiersicherheit)	besondere Ausrüstung (diese Angabe impliziert, dass "quasi nicht fälschbar" auch möglich ist)
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	silikonartig
	Ort des Sicherheitsmerkmals (Bauraum)	sehr begrenzter Bauraum, dennoch voluminöse Markierung möglich
	Belastungen am Einbauort	abrasive Prozesse, Verschmutzungen durch Verpackungsgut, Beschleunigungen und Schwingungen, lipophile Stoffe (Minimalschmierung, Verpackungsgut), starke Reinigungsmittel, hohe Luftfeuchtigkeit
	Distanz bei der Prüfung	> 0 mm möglich, situations- & konstruktionsabhängig
	Prüfaufwand (Prüfzeit)	0 s bei automatischer Prüfung, d. h. Authentifizierung im laufenden Betrieb
	Sicherheit (Manipulationssicherheit)	nicht manipulierbar, d. h. selbstzerstörend bei einem Manipulationsversuch
	Sicherheit (Belastbarkeit der Authentifizierung)	Das System sollte einen Mehrwert für Kunden, interne Überprüfungen der Originalität sowie einen gerichtsverwertbaren Nachweis der Originalität ermöglichen.
	Branding	gerne, falls möglich
	Backup-Prüfung	keine

Tabelle 7-4: Angaben der Vollmer Werke Maschinenfabrik GmbH für die Einmesslehre bzgl. der Auswahlkriterien

	Vollmer Werke Maschinenfabrik GmbH: Einmesslehre	
	Kriterium	**angegebene Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	Produkt
	Authentifizierungshäufigkeit	unbegrenzt
	Authentifizierungsinformation	Unikatkennzeichen
	Weitere Daten	ja
	Zugänglichkeit bei der Prüfung	berührend (diese Angabe impliziert, dass „berührungslos“ auch möglich ist)
	Infrastruktur für Prüfung	offline, d.h. Strom vorhanden, „keine“ ebenfalls möglich
	Prüfaufwand (Hilfsmittel)	portabel oder festinstalliert
	Automatisierungsgrad der Prüfung	halbautomatisch oder automatisch an der Maschine
Kriterien zur Bewertung	Variable Daten	nein (inkludiert ebenfalls Technologien, bei denen ein "ja" angegeben ist)
	Verbindung zwischen Sicherheitsmerkmal und Produkt	alle Verbindungsmöglichkeiten außer „Einbringen“
	Sicherheit (Kopiersicherheit)	besondere Ausrüstung (diese Angabe impliziert, dass "quasi nicht fälschbar" auch möglich ist)
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	metallisch, Werkzeugstahl
	Ort des Sicherheitsmerkmals (Bauraum)	flächige, auftragende Markierung möglich
	Belastungen am Einbauort	lipophile Stoffe (Öle, Kühlschmiermittel), hohe Luftfeuchtigkeit, magnetische und elektrische Energiedichte, Verschmutzung, Scheuern
	Distanz bei der Prüfung	≥ 0 mm, situations- & konstruktionsabhängig
	Prüfaufwand (Prüfzeit)	< 60 s
	Sicherheit (Manipulationssicherheit)	wenigstens sollte für einen Manipulationsversuch Spezialausrüstung notwendig sein
	Sicherheit (Belastbarkeit der Authentifizierung)	Das System sollte einen Mehrwert für Kunden, interne Überprüfungen der Originalität sowie einen gerichtsverwertbaren Nachweis der Originalität ermöglichen.
	Branding	ja
	Backup-Prüfung	keine

Tabelle 7-5: Angaben der Vollmer Werke Maschinenfabrik GmbH für die Drahttransportrolle bzgl. der Auswahlkriterien

	Vollmer Werke Maschinenfabrik GmbH: Drahttransportrolle	
	Kriterium	**angegebene Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	Produkt
	Authentifizierungshäufigkeit	unbegrenzt
	Authentifizierungsinformation	Originalitätskennzeichen
	Weitere Daten	nein (inkludiert ebenfalls Technologien, bei denen ein "ja" angegeben ist)
	Zugänglichkeit bei der Prüfung	berührend (diese Angabe impliziert, dass „berührungslos“ auch möglich ist)
	Infrastruktur für Prüfung	keine
	Prüfaufwand (Hilfsmittel)	keine
	Automatisierungsgrad der Prüfung	manuell
Kriterien zur Bewertung	Variable Daten	nein (inkludiert ebenfalls Technologien, bei denen ein "ja" angegeben ist)
	Verbindung zwischen Sicherheitsmerkmal und Produkt	alle Verbindungsmöglichkeiten außer „Einbringen“
	Sicherheit (Kopiersicherheit)	„einfache Hilfsmittel“ (diese Angabe impliziert, dass „besondere Ausrüstung“ und „quasi nicht fälschbar“ auch möglich sind)
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	metallisch, Aluminium
	Ort des Sicherheitsmerkmals (Bauraum)	flächige Markierung möglich
	Belastungen am Einbauort	lipophile Stoffe (Öle, Kühlschmiermittel), hohe Luftfeuchtigkeit
	Distanz bei der Prüfung	≥ 0 mm, situations- & konstruktionsabhängig
	Prüfaufwand (Prüfzeit)	< 60 s
	Sicherheit (Manipulationssicherheit)	wenigstens sollte für einen Manipulationsversuch Spezialausrüstung notwendig sein
	Sicherheit (Belastbarkeit der Authentifizierung)	Das System sollte einen Mehrwert für Kunden, interne Überprüfungen der Originalität sowie einen gerichtsverwertbaren Nachweis der Originalität ermöglichen.
	Branding	ja
	Backup-Prüfung	keine

7.1.3.2 Ergebnisse des Auswahlprozesses von je schützenswertem Bauteil passenden Sicherheitsmerkmalen

Das Ergebnis aus dem Auswahlprozess nach Abschnitt 7.1.2 mit den Angaben aus Abschnitt 7.1.3.1 ist in den folgenden Tabellen abgebildet.

Tabelle 7-6: Ergebnistabellen zu den Beispielen im Abschnitt 7.1.3.1 mit zugehöriger Legende (die Tabellen tragen passende Überschriften für eine klare Zuordnung zu den Ursprungsangaben in Abschnitt 7.1.3.1)

Legende	
Text	Kriterien für die Auswahl geeigneter Sicherheitsmerkmale
Text	Ausprägungen aufgrund der Anforderungen durch das Bauteil, dessen Umgebung bzw. des beauftragenden Unternehmens für Auswahlkriterien
Text	Kriterien zur Bewertung
Text	Ausprägungen aufgrund der Anforderungen durch das Bauteil, dessen Umgebung bzw. des beauftragenden Unternehmens für Bewertungskriterien

Multivac: Klammerkette

Sicherheitsmerkmale		Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)										
		Daten			Anbringung		Prüfung des Kennzeichens					Sicherheit
		Authenti-fizierungs-information	Weitere Daten	Variable Daten	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
		Originalität [1]	ja [3]	ja [4]	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
		Unikat [2]	nein	nein	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
						OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
						OA [8]				Labortechnik [16]	labortech. [21]	
Kennz. / Techn. / System	**Abschnitt**					ET [9]						
Radiofrequenzidentifikation (RFID)	A.3.6	Unikat	ja	ja	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
Rauschmustercodes	A.5.5.5	Unikat	ja	nein	beides	OA / ET	unbegrenzt	ber.los	Strom / Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.

Multivac: Siegeldichtung

Sicherheitsmerkmale		Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)										
		Daten			Anbringung		Prüfung des Kennzeichens					Sicherheit
		Authenti-fizierungs-information	Weitere Daten	Variable Daten	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
		Originalität [1]	ja [3]	ja [4]	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
		Unikat [2]	nein	nein	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
						OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
						OA [8]				Labortechnik [16]	labortech. [21]	
Kennz. / Techn. / System	**Abschnitt**					ET [9]						
Radiofrequenzidentifikation (RFID)	A.3.6	Unikat	ja	ja	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
Rauschmustercodes	A.5.5.5	Unikat	ja	nein	beides	OA / ET	unbegrenzt	ber.los	Strom / Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.

Vollmer: Drahttransportrolle

Sicherheitsmerkmale		Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)											
		Daten			Anbringung		Prüfung des Kennzeichens					Sicherheit
		Authenti-fizierungs-information	Weitere Daten	Variable Daten	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
		Originalität [1]	ja [3]	ja [4]	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
		Unikat [2]	nein	nein	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
						OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
						OA [8]				Labortechnik [16]	labortech. [21]	
Kennz. / Techn. / System	**Abschnitt**					ET [9]						
Hochdruck	A.4.1.1	Originalität	nein	nein	beides	OA /ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
Tiefdruck	A.4.1.3	-	-	-	-	-	-	-	-	-	-	-
Intagliodruck / Stichtiefdruck	A.4.1.3.1	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
Orlof-Technik / Schablonen-einfärbetechnik	A.4.1.3.2	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
Rastertiefdruck	A.4.1.3.3	Originalität	nein	nein	beides	OA / ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
Siebdruck	A.4.1.4	Originalität	nein	nein	beides	OÄ	unbegrenzt	berührend	keine	keine	manuell	besondere A.
Blindprägung	A.4.2.1	Originalität	nein	nein	beides	OÄ	unbegrenzt	berührend	keine	keine	manuell	besondere A.
Heißfolienprägung	A.4.2.2	Originalität	nein	nein	beides	ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
Hologramme	A.5.1.3	Originalität	nein	nein	beides	EI / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel	manuell / halbaut.	besondere A. / q. n. f.
Parallaxe	A.5.1.5	Originalität	nein	nein	beides	ET	unbegrenzt	ber.los	keine	keine	manuell	q. n. f.
Anti-Kopier-Muster	A.5.2.1	beides [25]	ja [26]	nein	beides	OA / ET [29]	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
Besondere Schriftart	A.5.2.2	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
Mikrotext	A.5.2.4	Originalität	nein	nein	beides	ET	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
Guillochen	A.5.3.1	Originalität	nein	nein	beides	ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
Irisdruck / Regenbogendruck	A.5.3.2	Originalität	nein	nein	beides	ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
⋮	⋮	⋮			⋮		⋮					⋮

...	...	...	...	...	...	...	...	...	...	...	...
Clustermerkmal	A.5.4.1	Originalität	nein	nein	beides	ET	unbegrenzt	ber.los	keine / Strom	keine/portabel	manuell / halbaut.	besondere A.
Fluoreszenz	A.5.4.3	-	-	-	-	-	-	-	-	-	-	-
Tagesleuchtfarbe / Neonfarbe als Echtfarbelement	A.5.4.3.3	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
Interferenz- und Effektfarbe	A.5.4.4	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
Kippfarbe / optisch variable	A.5.4.5	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
Sonderfarbe	A.5.4.14	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
thermoreaktive Farbe	A.5.4.16	-	-	-	-	-	-	-	-	-	-	-
Thermochrome Pigmente	A.5.4.16.2	Originalität	nein	nein	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel	manuell	besondere A.
Feuchtstempelabdruck	A.5.5.1	Originalität	nein	nein	beides	OA /ET	unbegrenzt	ber.los	keine	keine	manuell	einfache H.
Sicherheitsanstanzung	A.5.5.6	Originalität	nein	nein	beides	EI / ET [30]	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
Sicherheitsfaden	A.5.5.7	Originalität	nein	nein	beides	EI / ET [30]	unbegrenzt	ber.los	keine	keine	manuell	besondere A.

Vollmer: Einmesslehre

Sicherheitsmerkmale		Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)											
		Daten			Anbringung		Prüfung des Kennzeichens					Sicherheit
		Authenti-fizierungs-information	Weitere Daten	Variable Daten	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
		Originalität [1]	ja [3]	ja [4]	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
		Unikat [2]	nein	nein	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
						OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
						OA [8]				Labortechnik [16]	labortech. [21]	
Kennz. / Techn. / System	**Abschnitt**					ET [9]						
Radiofrequenzidentifikation (RFID)	A.3.6	Unikat	ja	ja	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
Rauschmustercodes	A.5.5.5	Unikat	ja	nein	beides	OA / ET	unbegrenzt	ber.los	Strom / Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.

Homag: Aggregate / HSK-Schnittstelle

Sicherheitsmerkmale		Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)											
		Daten			Anbringung		Prüfung des Kennzeichens					Sicherheit
		Authenti-fizierungs-information	Weitere Daten	Variable Daten	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
		Originalität [1]	ja [3]	ja [4]	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
		Unikat [2]	nein	nein	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
						OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
						OA [8]				Labortechnik [16]	labortech. [21]	
Kennz. / Techn. / System	**Abschnitt**					ET [9]						
Radiofrequenzidentifikation (RFID)	A.3.6	Unikat	ja	ja	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
Rauschmustercodes	A.5.5.5	Unikat	ja	nein	beides	OA / ET	unbegrenzt	ber.los	Strom / Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.

7.2 Auswahl von Sicherheitsmerkmalen aufgrund wirtschaftlicher Rahmenbedingungen

In Abschnitt „7.1 Auswahl von Sicherheitsmerkmalen aufgrund technischer Rahmenbedingungen“ wurde die Menge an prinzipiell möglichen Sicherheitsmerkmalen bestimmt, bewertet und Vorarbeit für die Feinplanung und Ausgestaltung geleistet. Nun ist auch die wirtschaftliche Seite der Nutzung der Sicherheitsmerkmale zu untersuchen (siehe Abbildung 7-1).

Diese erfolgt im Vorgriff auf die detaillierte Darstellung des Gesamtsystems zur Kennzeichnung und Authentifizierung von Komponenten und Ersatzteilen im Maschinen- und Anlagenbau in Kapitel 8. Obwohl somit noch nicht dargestellt ist, welche Komponenten für ein passendes Gesamtsystem benötigt werden, soll hier dennoch das methodische Vorgehen zur Bewertung auf Basis wirtschaftlicher Kriterien entwickelt werden. Dies erfolgt auch im Vorgriff darauf, welche Wirkungsweise das Gesamtsystem im Markt erreichen kann. Denn es sind beispielsweise kundenspezifische Zusatznutzen, die im Gesamtsystem integriert werden können, noch nicht bekannt oder implemeniert (siehe Kapitel 9, S. 215). Diese Kenntnis ist jedoch Voraussetzung für valide Abschätzungen, welche für eine wirtschaftliche Betrachtung notwendig sind.

7.2.1 Wirtschaftliche Auswahlkriterien

Prinzipiell handelt es sich bei der Einführung und Verwendung von Sicherheitsmerkmalen um eine Investition, welche der Originalhersteller tätigt. Ziel einer Investition ist es, den langfristigen Gewinn zu maximieren. Dieser Investitionserfolg kann in entsprechenden Investitionsplanungsmodellen abgebildet und so die Sinnhaftigkeit der Investition gezeigt werden [Wöh-05 S. 583 ff.]. Dies sollte auch im Falle der Einführung von Sicherheitsmerkmalen auf Originalbauteilen und einer Infrastruktur zur Prüfung dieser Merkmale erfolgen.

Um die Wirtschaftlichkeit dieser Investition im Vorhinein zu überprüfen, könnten sämtliche bekannten Verfahren der Investitionsrechnung verwendet werden [siehe beispielsweise Gün-13a, VDI2693, Wöh-05 S. 583 ff.]. Dabei sind für die Bewertung der Wirtschaftlichkeit einer Investition die folgenden Eingangsdaten notwendig: Anschaffungs- bzw. Herstellungskosten, die durch die Investition zusätzlich zu erzielenden laufenden Einnahmeüberschüsse, verringert durch die laufenden Kosten aus der betreffenden Investition [in Anlehnung an VDI2693].

Die Investitionsausgaben für ein entsprechendes Gesamtsystem können mit Hilfe von Angeboten sehr genau ermittelt werden. Hierzu gehören beispielsweise einmalige Werkzeugkosten für die Produktion eines individuellen Sicherheitsmerkmals und gegebenenfalls Anschaffungskosten für Prüfgeräte und eine passende Infrastruktur, eine Applikationseinrichtung für die Produktion sowie Schulungen für Mitarbeiter der Produktion, Logistik und des Vertriebs.

Die laufenden Kosten, die mit jedem Auf- / Einbringen eines Sicherheitsmerkmals auf / in ein Produkt verbunden sind, lassen sich in Zusammenarbeit mit anbietenden Unternehmen ebenfalls sehr genau bestimmen. Hierbei sind die Kosten je Sicherheitsmerkmal und die Kosten für den Kennzeichnungsvorgang selbst beinhaltet.

Sehr schwierig ist jedoch die Ermittlung der zu erwartenden laufenden Einnahmeüberschüsse. Die laufenden Einnahmeüberschüsse aufgrund der Einführung von Sicherheitsmerkmalen ergeben sich daraus, dass die für Hersteller in Abschnitt 2.3.1, S. 19 genannten Schadensarten reduziert oder sogar eliminiert werden können. Bei Prüfung dieser Schadensarten muss jedoch festgestellt werden, dass nur wenige dieser Positionen wirklich monetär bewertbar sind.

Eine Einschätzung, welche Schadensarten prinzipiell in einer Wirtschaftlichkeitsbetrachtung als monetär erfassbar oder schätzbar und welche Schadensarten als sehr

schwierig monetär zu bewerten eingestuft werden, wird in Tabelle 7-7 für den Ist-Zustand und Tabelle 7-8 für den Plan-Zustand gegeben. Diese Tabellen sind aus logischer Überlegung sowie aus Experteninterviews [Fuc-13, Mei-13, Sim-13] entstanden. Der Ist-Zustand bezieht sich dabei auf den aktuellen Zustand in einem Unternehmen und die feststellbaren Schäden aufgrund von Produkt- und Markenpiraterie bevor ein Sicherheitsmerkmal und zugehörige Infrastruktur eingeführt werden. Der Plan-Zustand wird in der Zeit nach Einführung eines Sicherheitsmerkmals erreicht. Dabei ist besonders schwierig abzuschätzen, wie die Wirkung dieser Maßnahme auf die Verringerung der Schäden sein wird.

Tabelle 7-7: Schadensarten aus Abschnitt 2.3.1, S. 19 und Einschätzung der monetären Bewertbarkeit im Ist-Zustand

Nr.	Schadensarten	Kosten / Schaden monetär erfassbar	Kosten / Schaden schätzbar	sehr schwierig monetär zu bewerten	Begründung
	Unmittelbare Schadensarten				
1	Umsatz- und Gewinnverluste	x	x		Zur Herleitung der Umsatz- und Gewinnverluste aufgrund von Produkt- und Markenpiraterie gibt es nach *Fuchs und Zhou* drei mögliche Wege [Fuc-09]. Für den Maschinen- und Anlagenbau ist in Abschnitt 7.2.2.1 eine vierte Möglichkeit auf Basis der Maschinen im Feld dargestellt. Teilweise sind die Wirkungen von Produkt- und Markenpiraterie jedoch nicht trennscharf von anderen Wettbewerbsfaktoren erfassbar.
2	Verminderte Einnahmen der Rechteinhaber aus Lizenzgebühren		x	x	Die Basis für die Umsatz- und Gewinnverluste bilden Absatzzahlen für Ersatzteile und Komponenten. Der Wert für die Vergabe von Lizenzen für deren Produktion kann somit geschätzt werden. In manchen Fällen sind diese Zahlen jedoch wenig belastbar herzuleiten und die Anzahl erzeugter Kopien am Weltmarkt bleibt unklar. Damit wäre auch die Anzahl möglicher Lizenzen und deren Wert aufgrund des unbekannten Volumens schwer zu beziffern.
3	Kosten für Anmeldung, Verfolgung und Durchsetzung von Schutzrechten	x	x		Die Kosten für diese Aktivitäten eines Unternehmens sind aus Vergangenheitswerten und somit zum Planungszeitpunkt bekannt. Die laufenden Kosten für Verfolgung und Durchsetzung zum Planungszeitpunkt sind allerdings nur schwer erfassbar. Unwägbarkeiten sind z. B. schleppende Ermittlungsergebnisse, unklare Ausgänge von Gerichtsverfahren, eventuelle Berufungen oder Revisionen, tatsächlicher Schadenersatz.
4	Kosten für Schutzmaßnahmen	x			Die Kosten für diese Aktivitäten eines Unternehmens sind zum Planungszeitpunkt bekannt.
	Mittelbare Schadensarten				
5	Druck auf das Preisniveau und Preisverfall		x		In vielen Fällen ist der Preisverfall aufgrund der Existenz von Kopien auf den Märkten über mehrere Jahre für Fachexperten ersichtlich und nachvollziehbar und der Schaden somit abschätzbar.
6	Imageverlust, Erosion der Marken und des Unternehmenswerts	x		x	Die Berechnung der langfristigen Erosion der Marke erfolgt nach *Fuchs und Zhou* [Fuc-09]. Die Auswirkungen von existierenden Kopien auf das Image bzw. den Unternehmenswert ist kaum oder lediglich mit sehr großem Aufwand isoliert feststellbar.
7	Kosten für ungerechtfertigte Kundendiensteinsätze, Gewährleistungsansprüche, Garantieforderungen	x			Die Kosten für diese Aktivitäten eines Unternehmens sind zum Planungszeitpunkt bekannt.
8	Kosten für die begründete Ablehnung von Forderungen aufgrund Verfügbarkeitsgarantien, Regressforderungen und Produkthaftungsansprüchen	x			Die Kosten für diese Aktivitäten eines Unternehmens sind zum Planungszeitpunkt bekannt.
9	Verlust eigenen Know-hows			x	Die Auswirkungen dieser negativen Konsequenzen von Produkt- und Markenpiraterie auf beispielsweise Umsatz oder Gewinn sind nur schwierig oder gar nicht abzuleiten. Diese Positionen sind daher monetär kaum oder gar nicht bewertbar.
10	Verlust des Know-how- und Innovationsvorsprungs			x	
...	...	...	...	...	...

...		...	...	...	...
...	**Mittelbare Schadensarten**				
11	Verlust von Marktanteilen	x	x		Nach *Fuchs und Zhou* ist hier die Berechnung des Barwerts der Umsatzverluste aus dem Verlust dieser Marktanteile entscheidend [Fuc-09]. Dieser kann jedoch teilweise nicht trennscharf von anderen Wettbewerbsfaktoren erfasst werden.
12	Verlust von Absatzmärkten	x	x		In manchen Fällen wurde der Markt eines Originalherstellers über mehrere Monate schleichend, aber schließlich komplett durch Fälscher und Kopierer übernommen, der Originalhersteller hat kaum noch Marktanteile. In diesen Fällen kann der Verlust relativ genau beziffert werden [Fuc-09]. In anderen Fällen kann es sehr schwierig sein, den Anteil von Produkt- und Markenpiraterie am Verlust des Absatzmarktes von anderen Wettbewerbsfaktoren getrennt abzubilden.
13	Verlust von Zukunftsmärkten		x	x	In gewissen Fällen, in denen gesicherte Informationen über die Wettbewerbssituation in einem anvisierten Zukunftsmarkt vorliegen und der Erfolg teilweise oder gänzlich aufgrund von Produkt- und Markenpiraterie in Frage gestellt wird, kann dieser Schaden monetär bewertet werden. Liegen diese Informationen nicht vor und ist die Wettbewerbssituation auf einem Zukunftsmarkt bezüglich redlicher, aber insbesondere auch unredlicher Wettbewerber unbekannt, kann auch nicht abgeleitet werden, welche Umsatz- und Gewinnverluste zu erwarten sind. Dies kann somit in bestimmten Fällen durch eine sehr detaillierte Recherche auf Einzelmärkten festgestellt werden und ist dann über zukünftige Umsatz- und Gewinnverluste abbildbar.
14	Negative Auswirkungen auf Forschung und Entwicklung sowie andere kreative Aktivitäten			x	Da schwer abschätzbar ist, welchen Beitrag aktuelle Investitionen in Forschung und Entwicklung auf zukünftige Umsatz- und Gewinnentwicklungen in einem Unternehmen haben, ist auch die Verringerung der Aktivitäten in diesem Bereich und deren negative Auswirkungen schwer zu beziffern.
15	Verringerung der Unternehmensinvestitionen		x	x	Verschiedene Unternehmensinvestitionen sind bezüglich ihrer Auswirkungen auf Umsatz und Gewinn verschieden konkret monetär bewertbar. Je nach Konkretisierung dieser Auswirkung kann dies in die Kalkulation einbezogen werden. Andernfalls ist das nur schwer möglich. Bei Verringerung der Unternehmensinvestitionen sind jedoch in jedem Fall Nachteile in der Wettbewerbsfähigkeit die Folge.
16	Verlangsamung des eigenen technischen Fortschritts			x	Da schon die "negativen Auswirkungen auf Forschung und Entwicklung sowie andere kreative Aktivitäten" kaum zu bewerten sind, kann auch die Verlangsamung des eigenen technischen Fortschritts kaum beziffert werden. Als Folge sind jedoch Nachteile in der Wettbewerbsfähigkeit absehbar.
17	Schwächung der eigenen Wettbewerbsfähigkeit			x	Zwar können die Positionen (11) und (12) relativ gut abgebildet werden, die negativen Auswirkungen auf die Positionen wie (13), (15) oder (16) jedoch sind kaum oder gar nicht zu beziffern. Daher kann auch diese Position als aus diesen Größen abgeleitete Position nur sehr vage bestimmt werden.
18	Einschränkung der Geschäftstätigkeit der Rechteinhaber, erhöhtes Konkursrisiko		x	x	Abhängig von der Bewertung der anderen Positionen (11), (12), (13), (15), (16) bzw. (17) kann diese Position als aus diesen Größen abgeleitet teilweise abgebildet werden. Sind diese genannten Positionen jedoch nicht bestimmbar, kann auch die "Einschränkung der Geschäftstätigkeit der Rechteinhaber, erhöhtes Konkursrisiko" bzw. "Insolvenz" als aus diesen Größen abgeleitete
19	Insolvenz		x	x	Position nicht beziffert werden.
20	Haftung wegen unterlassener Pirateriebekämpfung		x		In der Rechtsprechung existieren bereits Fälle, in denen Wirtschaftsbeteiligte im Vertriebsnetz des Originalherstellers haftbar gemacht wurden [siehe Ste-11a S. 71, Wel-07 S. 49 ff., Uni-04]. Da Originalhersteller zumindest nach US-Rechtsprechung in diesem Fall für Schäden aus Kopien nicht haftbar gemacht werden können, ist diese Position zwar ein denkbarer Schaden im Ist-Zustand, aber aus heutiger Sicht eher theoretisch.

Tabelle 7-8: Schadensarten aus Abschnitt 2.3.1, S. 19 und Einschätzung der monetären Bewertbarkeit im Plan-Zustand

Nr.	Schadensarten	Kosten / Schaden monetär erfassbar	Kosten / Schaden schätzbar	sehr schwierig monetär zu bewerten	Begründung
	Unmittelbare Schadensarten				
1	Umsatz- und Gewinnverluste		x	x	Die Wirkung des Einsatzes von Sicherheitsmerkmalen ist sehr stark technologie- und systemabhängig. Eine fundierte Schätzung der fallspezifischen Wirkung kann in bestimmten Fällen mit Hilfe der anbietenden Unternehmen und existierenden Beispielen abgeschätzt werden. In diesem Fall ist die Reduktion der Umsatz- und Gewinnverluste im Plan-Zustand mit Hilfe von Schätzungen herleitbar. Dieser Weg kann jedoch nicht immer beschritten werden.
2	Verminderte Einnahmen der Rechteinhaber aus Lizenzgebühren		x	x	Die Basis für die Umsatz- und Gewinnverluste bilden Absatzzahlen für Ersatzteile und Komponenten. Diese Absatzzahlen lassen sich prognostizieren und somit auch der Wert für die Vergabe von Lizenzen für deren Produktion. In manchen Fällen sind diese Zahlen jedoch wenig belastbar herzuleiten und die Anzahl erzeugter Kopien am Weltmarkt bleibt unklar. Damit wäre auch die Anzahl möglicher Lizenzen und deren Wert aufgrund des unbekannten Volumens schwer zu beziffern.
3	Kosten für Anmeldung, Verfolgung und Durchsetzung von Schutzrechten		x	x	Die Auswirkung der Einführung eines Sicherheitsmerkmals auf diese Kosten lässt sich bestenfalls abschätzen. Jedoch sind diese Schätzungen äußerst unsicher, da es nicht möglich ist, vorher zu sagen, wie viele momentane oder potenzielle neue Fälscher durch die Einführung eines Sicherheitsmerkmals vom Kopieren abgehalten werden. Auch könnten durch die Einführung des Sicherheitsmerkmals neue Kosten in diesem Bereich entstehen, da durch ein Sicherheitsmerkmal Fälscher aufgedeckt werden, die vorher noch nicht bekannt waren.
4	Kosten für Schutzmaßnahmen	x			Die Kosten für den Invest in Sicherheitsmerkmale sowie die laufenden Kosten dafür sind in der Planungsphase in Zusammenarbeit mit den anbietenden Unternehmen sehr gut zu beziffern.
	Mittelbare Schadensarten				
5	Druck auf das Preisniveau und Preisverfall		x	x	Die Wirkung des Einsatzes von Sicherheitsmerkmalen ist sehr stark technologie- und systemabhängig. In Zusammenarbeit mit den anbietenden Unternehmen kann zwar die Wirkungsweise aufgezeigt werden, wie diese sich auf das Preisniveau auswirkt, ist jedoch äußerst schwierig abzuleiten. Die Erfahrung zeigt jedoch, dass bei Einführung eines Sicherheitsmerkmals der Druck auf das eigene Preisniveau sinkt, da der Kunde sicher ist, ein Original zu erwerben. Der Zwang, mit den niedrigen Preisen redlicher oder unredlicher Konkurrenten mithalten zu müssen, entfällt.
6	Imageverlust, Erosion der Marken und des Unternehmenswerts		x	x	Die Wirkung des Einsatzes von Sicherheitsmerkmalen ist sehr stark technologie- und systemabhängig. In Zusammenarbeit mit den anbietenden Unternehmen kann evtl. auf Basis existierender Beispiele die Wirkung auf den Erhalt des Markenwerts abgeschätzt werden. Dies ist jedoch äußerst schwierig. Bezüglich des Images bzw. dem Unternehmenswert ist praktisch gesehen keine monetäre Bewertung möglich.
...	...	...	...	...	...

…	…	…	…	…
7	Kosten für ungerechtfertigte Kunden-diensteinsätze, Gewährleistungs-ansprüche, Garantieforderungen	x		Die Wirkung des Einsatzes von Sicherheitsmerkmalen könnte in der Planungsphase durch die Kosten für strittige Fälle im Bereich von Gewährleistung und Garantie abgeschätzt und monetär bewertet werden. Auch lässt sich in einer Nachkalkulation gut abbilden, welche Fälle aufgrund des eindeutigen Nachweises der Nicht-Originalität klar aus Gewährleistung und Garantie herausgenommen werden konnten. Dies setzt eine entsprechende Dokumentation im Vorfeld voraus.
8	Kosten für die begründete Ablehnung von Forderungen aufgrund Verfüg-barkeitsgarantien, Regressforde-rungen und Produkthaftungs-ansprüchen	x		Die Wirkung des Einsatzes von Sicherheitsmerkmalen könnte in der Planungsphase durch die Kosten für strittige Fälle im Bereich von Gewährleistung und Garantie abgeschätzt und monetär bewertet werden. Auch lässt sich in einer Nachkalkulation gut abbilden, welche Fälle aufgrund des eindeutigen Nachweises der Nicht-Originalität klar aus Gewährleistung und Garantie herausgenommen werden konnten. Dies setzt eine entsprechende Dokumentation im Vorfeld voraus.
9	Verlust eigenen Know-hows		x	Diese Positionen sind bereits im Ist-Zustand kaum monetär zu bewerten und somit im Plan-Zustand ebenso kaum herzuleiten.
10	Verlust des Know-how- und Innovationsvorsprungs		x	
11	Verlust von Marktanteilen	x		Die Reduktion des Verlusts von Marktanteilen durch die Einführung eines Sicherheitsmerkmals kann durch Experten des Vertriebs in Zusammenarbeit mit den Unternehmen, welche die entsprechenden Sicherheitsmerkmale anbieten, abgeschätzt werden. Diese Abschätzung mündet dann in die Verringerung des Umsatz- und Gewinnverlusts. Eine genaue Angabe der zurückgewonnenen Marktanteile ist äußerst schwierig herzuleiten, da bereits im Ist-Zustand die Anzahl an Kopien auf dem Weltmarkt oder deren zeitliche Entwicklung unbekannt sind - genaue Statistiken hierzu existieren nicht.
12	Verlust von Absatzmärkten	x		In diesem Extremfall könnte in der Planungsphase mit den anbietenden Unternehmen die Wirkungsweise des Einsatzes von speziellen Sicherheitsmerkmalen diskutiert werden, die sehr stark technologie- und systemabhängig ist. Aus Beispielen lässt sich jedoch eventuell ein Anteil am Absatzmarkt ableiten, den der Originalhersteller durch Einsatz dieser Sicherheitsmerkmale zurückgewinnen kann.
13	Verlust von Zukunftsmärkten		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
14	Negative Auswirkungen auf Forschung und Entwicklung sowie andere kreative Aktivitäten		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
15	Verringerung der Unternehmensinvestitionen		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
16	Verlangsamung des eigenen technischen Fortschritts		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
17	Schwächung der eigenen Wettbewerbsfähigkeit		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
18	Einschränkung der Geschäftstätigkeit der Rechteinhaber, erhöhtes Konkursrisiko		x	Diese Positionen sind bereits im Ist-Zustand sehr schwer monetär zu bewerten und somit im Plan-Zustand kaum herzuleiten.
19	Insolvenz		x	
20	Haftung wegen unterlassener Pirateriebekämpfung	x		Die Bewertung dieser Position kann evtl. aus vergleichbaren Fällen abgeleitet und somit der Größenordnung nach abgeschätzt werden [Ste-11a S. 71, Wel-07 S. 49 ff., Uni-04].

7.2.2 Zukünftige, zu erwartende laufende Einnahmeüberschüsse am Beispiel der Umsatz- und Gewinnverluste

Wie trotz dieser Schwierigkeiten und Hemmnisse die Herleitung der zu erwartenden laufenden Einnahmeüberschüsse methodisch gestützt und sinnvoll erfolgen kann, soll hier am Beispiel der Umsatz- und Gewinnverluste gezeigt werden. Diese zu bestimmen, ist teilweise nur mit Hilfe von Schätzungen möglich. Denn es ist zunächst unbekannt, welchen Marktanteil am After-Sales des betrachteten schützenswerten Bauteils redliche sowie unredliche Wettbewerber vor Einführung von Sicherheitsmerkmalen haben.

Wie *Fuchs und Zhou* darstellen, können die Umsatz- und Gewinnverluste im Ist-Zustand jedoch auf drei verschiedenen Wegen hergeleitet werden [Fuc-09]:

- Berechnung aus Branchenwerten
- Hochrechnung einzelner Fälle
- Berechnung über den Umsatz der Fälscher

Die Anwendung eines weiteren Verfahrens, das im speziellen Fall des Maschinen- und Anlagenbaus möglich ist, wird im nächsten Abschnitt detailliert dargestellt.

Schwieriger wird es bei der Abschätzung der Wirkung, welche die Einführung eines Sicherheitsmerkmals inklusive des Systems zur Authentifizierung der markierten Originalbauteile hat. Hierzu gibt es bei den Unternehmen, die entsprechende Sicherheitsmerkmale anbietenden, Erfahrungswerte aus Einzelprojekten. Diese sind zwar aufgrund der spezifischen Rahmenbedingungen im jeweiligen Einzelfall nicht verallgemeinerbar, aber teilweise mit entsprechenden Überlegungen und Argumentationen auf den jeweiligen konkreten vorliegenden Fall übertragbar.

Im Folgenden wird dargestellt, wie im Maschinen- und Anlagenbau die Marktaufteilung zwischen Originalhersteller und Kopierern im Ist- wie auch im Plan-Zustand hergeleitet und bewertet werden kann.

7.2.2.1 Ist-Zustand

Geht man davon aus, dass sich der Markt für ein schützenswertes Bauteil im Ist-Zustand aufteilt in Originalbauteile und Kopien, können deren Marktanteile näherungsweise bestimmt werden. Ergänzend zu den drei oben genannten Herleitungs-

möglichkeiten wird hier eine weitere Möglichkeit dargestellt, diese Marktanteile zu bestimmen.

Ein Originalhersteller kann basierend auf der Anzahl der im Feld befindlichen Maschinen, in denen das betrachtete schützenswerte Bauteil eingesetzt wird, und dem aus Vergangenheitswerten bekannten Bedarf pro Jahr, der aus dem Verschleiß dieses Bauteils u. Ä. resultiert, relativ genau bestimmen, wie groß die rechnerisch benötigte Stückzahl für ein Bauteil im After-Sales pro Jahr N_G ist. Andererseits kennt der Originalhersteller die pro Jahr verkaufte Stückzahl des Originalbauteils N_o. Die pro Jahr durch redliche oder unredliche Wettbewerber verkaufte Stückzahl an Kopien N_K ergibt sich rechnerisch aus dem Zusammenhang:

$$N_G = N_o + N_K \tag{7-1}$$

Bei den Beispielunternehmen (siehe Abschnitt 5.2.2, S. 89) konnten diese Stückzahlen für einzelne Bauteile beispielhaft ermittelt werden. Dabei ergaben sich für die Marktanteile, die durch Kopien eines betrachteten Bauteils abgeschöpft werden, zwischen 10 % und 50 %. Ein Originalanbieter, der einen Marktanteil für Kopien mit ca. 50 % annimmt und selbst pro Jahr N_o = 77.000 Stück des Originalbauteils vertreibt, geht somit davon aus, dass ca. N_K = 77.000 Kopien pro Jahr von redlichen oder unredlichen Wettbewerbern verkauft werden (siehe Abbildung 7-7). Diese Marktaufteilung wurde für mehrere Bauteile von verschiedenen Firmen angeführt.

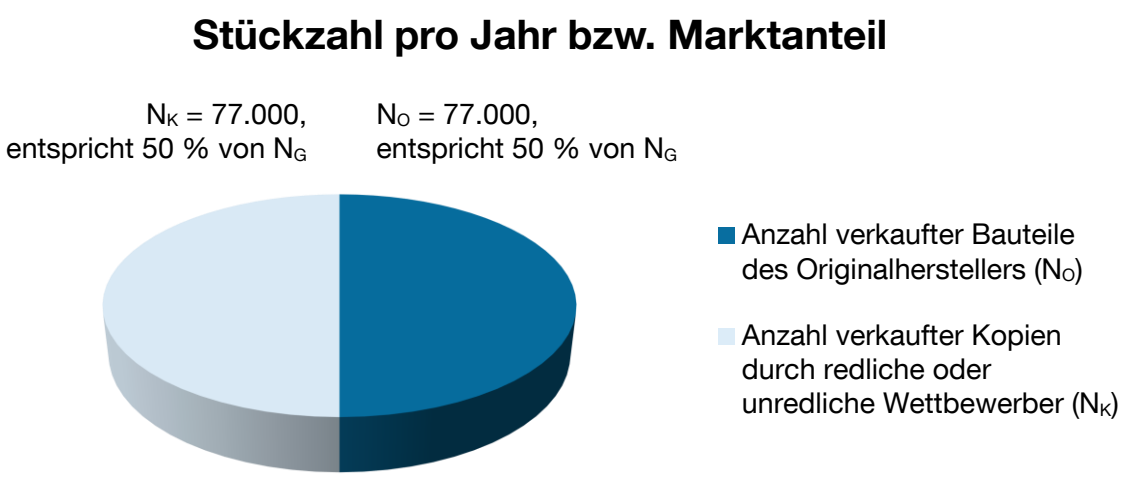


Abbildung 7-7: Beispiel einer Marktaufteilung für ein bestimmtes, von Produktpiraterie betroffenes, schützenswertes Bauteil [23]

[23] siehe Forschungsprojekt ProAuthent, Firma & Bauteil dürfen nicht konkret benannt werden

7.2.2.2 Plan-Zustand

Die Marktaufteilung deutet auf enormes Potenzial bezüglich der Steigerung des eigenen Umsatzes im After-Sales hin. Daher ist es von großem Interesse, für den Plan-Zustand den Anteil zu ermitteln, um welchen der eigene Umsatz gesteigert werden könnte, wenn ein bestimmtes Sicherheitsmerkmal eingeführt werden würde. Dies ist einerseits stark von den jeweiligen Kunden und deren Kaufverhalten abhängig, andererseits vom Sicherheitsmerkmal selbst und dem damit verbundenen Gesamtsystem. Um diesen Anteil anzunähern, wird das folgende Vorgehen vorgeschlagen.

Zunächst wird der stückzahlbezogene maximale Marktanteil, der zurückgewonnen werden kann, wenn ein Sicherheitsmerkmal eingeführt wird, seitens der After-Sales-Experten in Zusammenarbeit mit den Experten der Unternehmen, welche entsprechende Sicherheitsmerkmale anbieten, geschätzt. Dieser Anteil q_{max} bezieht sich auf N_K und kann maximal 100 % betragen. Bei den im Forschungsprojekt ProAuthent analysierten Bauteilen bewegte sich dieser Anteil in einem weiten Spektrum bis zu 90 %, da die Experten davon ausgehen, dass nicht jeder, der eine Kopie kauft, auch ein Original kaufen würde oder es unterschiedliche Austauschzyklen aufgrund des unterschiedlich schnellen Verschleißes gibt [Dol-13]. Damit lässt sich $N_{O,max}$ berechnen, das die maximal zurückzugewinnende Stückzahl pro Jahr aufgrund des maximal zurückzugewinnenden Marktanteils darstellt:

$$N_{O,max} = q_{max} * N_K \tag{7-2}$$

Da jedoch davon auszugehen ist, dass dieser maximal zurückzugewinnende Marktanteil bei unterschiedlicher Ausgestaltung des Schutzsystems verschieden ausfällt, muss dieser Anteil abhängig der prinzipiell möglichen Sicherheitsmerkmale und der Expertise der jeweiligen Anbieter dieser Sicherheitsmerkmale relativiert werden. Für diese auf das Schutzsystem bezogene Relativierung soll hier ein situationsabhängiger Wirkungsgrad anhand des Sicherheitsmerkmals η_s eingeführt werden. Die durch die Einführung eines Sicherheitsmerkmals und passenden Schutzsystems pro Jahr zusätzlich verkaufte Stückzahl an Originalbauteilen berechnet sich damit wie folgt:

$$N_{O,Z} = \eta_S * N_{O,max} = \eta_S * q_{max} * N_K \tag{7-3}$$

Geht nun ein Originalhersteller, der 77.000 Originalbauteile pro Jahr im After-Sales verkauft und einen Marktanteil von 50 % hat, davon aus, dass mit dem Einsatz von Sicherheitsmerkmalen ein maximaler Marktanteil von q_{max} = 30 % zurückzugewinnen

wäre, könnte dieser Originalhersteller im nächsten Jahr maximal $N_{O,max}$ = 23.100 (= 30 % * 77.000) Originalbauteile mehr verkaufen. Bei Einsatz einer bestimmten Sicherheitstechnologie und einem passenden technischen Gesamtsystem kann der jeweilige Anbieter aufgrund seiner Expertise den situationsabhängigen Wirkungsgrad seines Sicherheitsmerkmals einschätzen – beispielsweise 70 %. Somit wäre der zu erwartende zusätzliche Verkauf an Originalbauteilen im After-Sales bei Einsatz dieses Sicherheitsmerkmals $N_{O,Z}$ = 16.170 (= 70 % * 30 % * 77.000) Stück pro Jahr. Die durch redliche oder unredliche Wettbewerber verkaufte Stückzahl des Bauteils N_K reduziert sich damit auf:

$$N_{K,S} = N_K - N_{O,Z} \tag{7-4}$$

Im Beispiel ergibt sich $N_{K,S}$ = 60.830 (= 77.000 – 16.170). Der Gesamtzusammenhang ist in Abbildung 7-8 grafisch dargestellt.

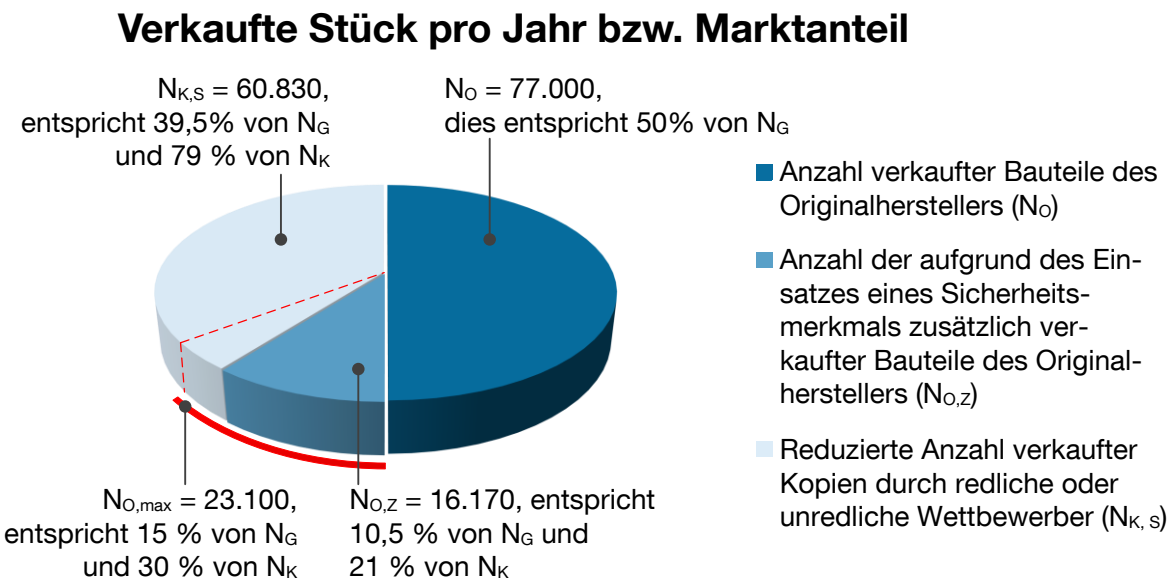


Abbildung 7-8: Beispiel einer abgeschätzten Marktaufteilung für das Bauteil nach Einführung eines Sicherheitsmerkmals, vergleiche hierzu Abbildung 7-7

Bei Bewertung dieser zusätzlich verkauften Bauteile $N_{O,Z}$ mit dem Verkaufspreis p, den der Originalhersteller pro verkauftem Bauteil realisiert, lässt sich der zu erwartende zusätzliche Umsatz $U_{O,Z}$ berechnen:

$$U_{O,Z} = p * N_{o,z} \tag{7-5}$$

Bei der Annahme des Preises p mit 30 € ergibt sich somit $U_{O,Z}$ zu 485.100 € (= 30 € * 16.170). Damit sind die folgenden Größen eingeführt und bestimmt:

N_G rechnerische Gesamtstückzahl eines Bauteils im After-Sales pro Jahr

N_O Anzahl verkaufter Bauteile des Originalherstellers pro Jahr

$N_{O,max}$ maximale Anzahl der aufgrund des Einsatzes von Sicherheitsmerkmalen durch den Originalhersteller zurückzugewinnende Stückzahl pro Jahr

$N_{O,Z}$ Anzahl der aufgrund des Einsatzes eines Sicherheitsmerkmals zusätzlich verkaufter Bauteile des Originalherstellers

N_K Anzahl verkaufter Kopien durch redliche oder unredliche Wettbewerber pro Jahr

$N_{K,S}$ reduzierte Anzahl der durch redliche oder unredliche Wettbewerber verkauften Kopien aufgrund des Einsatzes von Sicherheitsmerkmalen durch den Originalhersteller

q_{max} bezogen auf N_K maximaler Marktanteil, der zurückgewonnen werden könnte, wenn ein Sicherheitsmerkmal inklusive Gesamtsystem eingeführt werden würde

η_S situationsbezogener Wirkungsgrad eines Sicherheitsmerkmals

p Verkaufspreis, den der Originalhersteller pro verkauftem Bauteil realisiert

$U_{O,Z}$ der aufgrund des Einsatzes eines Sicherheitsmerkmals zu erwartende zusätzliche Umsatz pro Jahr

7.2.2.3 Szenariotechnik und Einsatz der Kapitalwertbestimmung

Die dargestellte Herleitung ist insbesondere im Blick auf N_K und $N_{O,Z}$ mit starken Unsicherheiten behaftet, da die Berechnungen auf Erfahrungswerten und Schätzungen basieren. Um die Einflüsse unterschiedlicher Einschätzungen der Ist-Situation im Parameter N_K bzw. der Wirkung des Produktpiraterie-Schutzsystems im Plan-Zustand im Parameter $N_{O,Z}$ abbilden zu können, gibt es verschiedene Möglichkeiten. Hier wird beispielhaft die Szenariotechnik herausgegriffen. Bei der Szenariotechnik handelt es sich um ein Planungsverfahren, bei dem mögliche alternative Entwicklungen (Szenarien) zur Gewinnung bedingter Vorhersagen erstellt und somit Chancen und Risiken von Entscheidungen besser abgeschätzt werden können [Bro-13c, Spr-12].

Ein Szenario bildet dabei Annahmen über Basisdaten und mögliche Abfolgen von Ereignissen des jeweils untersuchten Systemaspekts ab. In der Regel werden dafür mathematische Modelle verwendet, um beispielsweise eine Unternehmenssituation mit den relevanten zukünftigen Rahmenbedingungen in Form von Parametern zu

erfassen und zu verarbeiten (z. B. Modelle des Operations Research, ökonometrische Modelle). [Bro-13c]

Üblicherweise werden drei Szenarien entwickelt, die alle realistisch sein müssen und gleichzeitig die gesamte Bandbreite der Entwicklungsmöglichkeiten (Prognosekorridor) der untersuchten Situation erkennbar machen [Bro-13c, Spr-12]:

- Best-Case-Szenario als extrem optimistisches Szenario
- Worst-Case-Szenario als extrem pessimistisch Szenario
- Trend-Szenario als wahrscheinlichste Ausprägung

Übertragen auf die Frage, inwiefern sich die Investition in ein Produktpiraterie-Schutzsystem, wie es in der vorliegenden Arbeit vorgeschlagen wird, wirtschaftlich lohnt, können Szenarien entwickelt werden, um unterschiedliche zeitliche Entwicklungen und Einflüsse abzubilden.

Im vorliegenden Fall geht es um Schäden aus Produkt- und Markenpiraterie, die den Originalhersteller direkt oder indirekt betreffen (siehe Abschnitt 2.3.1, S. 19). Bei der Investition in Sicherheitsmerkmale inklusive dem passenden Gesamtsystem können diese Schäden reduziert und Neuumsätze durch etwaige neue Mehrwerte und Services für Kunden generiert werden (siehe Abschnitt 9.2, S. 224).

Dieser Zusammenhang ist sehr gut mit Hilfe der Kapitalwertmethode darstellbar, bei der über einen längeren zeitlichen Verlauf unterschiedliche Ein- und Auszahlungen für die einzelnen Perioden abgebildet werden können [Gün-13a]. Um die Wirtschaftlichkeit des Einsatzes von Sicherheitsmerkmalen und Gesamtsystem darstellen zu können, wird zunächst der Ist-Zustand erfasst, monetär bewertet und über die betrachtete Zeitspanne ohne Änderung fortgeschrieben. Danach wird der Plan-Zustand monetär bewertet und dem Ergebnis aus dem Ist-Zustand gegenüber gestellt. Die Ein- und Auszahlungen können dann je Periode verrechnet, mit einem passenden Zinssatz auf ihren Gegenwartswert in der Periode t=0 zurückgerechnet und addiert werden. Das Ergebnis ist der sogenannte Kapitalwert der Investition K_0.

Ist-Zustand

Die Vorgehensweise der Kapitalwertmethode wird bei der Abbildung des Ist-Zustands in Anlehnung an *Fuchs und Zhou* ergänzt, die in ihrer Veröffentlichung „Lohnt sich die Bekämpfung der Produkt- und Markenpiraterie?“ den Gesamtschaden für ein Unternehmen durch Produkt- und Markenpiraterie erstmals methodisch

fundiert monetär quantifiziert haben [Fuc-09]. Die am Ende des Abschnitts 7.2.2.2 zusammengefassten Größen werden dafür in den einzelnen Perioden fortgeschrieben. Zusätzlich werden in Abbildung 7-9 folgende Größen verwendet:

- t Zeitperiode
- $\hat{t}$ Zeithorizont: letzte Zeitperiode, welche in der Wirtschaftlichkeitsrechnung direkt und vollständig abgebildet wird
- U_G Gesamter Marktumsatz für das schützenswerte Bauteil, bildet den Umsatz des Originalherstellers ohne Schaden ab
- U_O Umsatz des Originalherstellers durch Verkauf der schützenswerten Bauteile pro Jahr
- $U_{O,verl}$ Umsatzverlust des Originalherstellers pro Jahr
- $G_{O,verl}$ Gewinnverlust des Originalherstellers pro Jahr
- g Gewinnspanne zur Abbildung des Gewinnverlusts als Anteil des Umsatzverlusts
- $CF_{statisch}$ statischer Cash-Flow-Verlust aufgrund des Gewinnverlusts des Originalherstellers pro Jahr
- $CF_{Barwert}$ Gegenwartswert des jährlichen Cash-Flow-Verlusts, somit auf die Periode t=0 abgezinster Cash-Flow-Verlust pro Jahr
- K_0 Gegenwartswert der jährlichen Verluste der betrachteten Perioden als Summe der $CF_{Barwert}$
- R_0 Fortschreibung der Verluste ab Periode t=8 und Gewichtung mit dem Gewichtungsfaktor r
- r Gewichtungsfaktor zur Gewichtung des Restwerts für die Zeitperioden ab t=8
- i Kapitalkostensatz
- $S_{0,gesamt}$ gesamter Produktpirateriesschaden für das betrachtete schützenswerte Bauteil als Barwert in t=0

Dabei wird das bisherige Beispiel aus den Abschnitten 7.2.2.1 und 7.2.2.2 fortgeschrieben mit folgenden Werten:

- $\hat{t} = 7$, somit ergibt sich t = 0, 1, … 7 als direkt betrachtete Perioden und t > 7 als indirekt betrachtete Perioden
- N_G = 154.000 Stück / Jahr
- N_O = 77.000 Stück / Jahr
- N_K = 77.000 Stück / Jahr
- p = 30 €

- g = 66 %
- r = 20 %
- i = 6 %

Ist-Zustand										
t		0	1	2	3	4	5	6	7	8
N_G	[Stück/Jahr]	154.000	154.000	154.000	154.000	154.000	154.000	154.000	154.000	
N_O	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
N_K	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
U_G	[Tsd. €]	4.620	4.620	4.620	4.620	4.620	4.620	4.620	4.620	
U_O	[Tsd. €]	2.310	2.310	2.310	2.310	2.310	2.310	2.310	2.310	
$U_{O,verl}$	[Tsd. €]	-2.310	-2.310	-2.310	-2.310	-2.310	-2.310	-2.310	-2.310	
$G_{O,verl}$	[Tsd. €]	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	
$CF_{statisch}$	[Tsd. €]	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	-1.525	
$CF_{Barwert}$	[Tsd. €]	-1.525	-1.438	-1.357	-1.280	-1.208	-1.139	-1.075	-1.014	-3.188

K_0 (ohne R_0)	[Tsd. €]	-10.035
R_0	[Tsd. €]	-3.188
$S_{0,gesamt}$	[Tsd. €]	-13.223

Abbildung 7-9: Beispiel für die Ermittlung des Gesamtschadens eines Unternehmens in Anlehnung an [Fuc-09], vergleiche hierzu Abbildung 7-7 und Abbildung 7-8

In Abbildung 7-9 sind folgende Formeln für die jeweilige Periode t angewendet:

$$U_G(t) = p * N_G(t) \tag{7-6}$$

$$U_O(t) = p * N_O(t) \tag{7-7}$$

$$U_{O,verl}(t) = U_G(t) - U_O(t) \tag{7-8}$$

$$G_{O,verl}(t) = g * U_{O,verl}(t) \tag{7-9}$$

$$CF_{statisch}(t) = G_{O,verl}(t) \tag{7-10}$$

$$CF_{Barwert}(t) = \begin{cases} \dfrac{CF_{statisch}(t)}{(1+\frac{i}{100})^t} & ,0 \le t \le \hat{t} \\ r * \sum_{t=\hat{t}+1}^{\infty} \dfrac{CF_{statisch}(\hat{t})}{\left(1+\frac{i}{100}\right)^t} & ,t = \hat{t}+1 \end{cases} \tag{7-11}$$

$$K_0 = \sum_{t=0}^{\hat{t}} CF_{Barwert}(t) \tag{7-12}$$

$$R_0 = CF_{Barwert}(\hat{t} + 1) \tag{7-13}$$

$$S_0 = K_0 + R_0 \tag{7-14}$$

Fuchs und Zhou gehen in ihrer Herleitung des Gesamtschadens im Ist-Zustand von einem permanenten Problem und damit einem jährlichen Schaden durch Produkt- und Markenpiraterie aus. Für den Betrachtungszeitraum von acht Perioden (also t = 0 .. 7) wird dieser Schaden konkret hergeleitet und beziffert. Für die nachfolgenden Perioden wird davon ausgegangen, dass das Problem weiterhin besteht. Aber dieser weit in der Zukunft liegende Schaden wird weniger stark bewertet. Dies wird durch die für $CF_{Barwert}$ für t = 8 (= $\hat{t}$ +1) hinterlegte Formel dargestellt.

Der gesamte Schaden aus Produkt- und Markenpiraterie für das betroffene Unternehmen hat unter den gemachten Annahmen in diesem Beispiel einen Gegenwartswert von $S_{0,gesamt}$ = 13,2 Mio € in Periode t = 0.

Um nun mittels der Kapitalwertmethode die Wirtschaftlichkeit der Investition in Sicherheitstechnologien und ein dazu passendes Gesamtsystem darzustellen, wird in den folgenden Abschnitten hergeleitet, wie sich die Verluste, also $S_{0,gesamt}$, aufgrund der Produkt- und Markenpiraterie für ein betroffenes Unternehmen reduzieren können. Da – wie bereits dargestellt – die Wirkung eines solchen Systems höchst unsicher ist, werden dafür mittels der Szenariotechnik verschiedene Szenarien abgebildet.

Best-Case-Szenario

Zunächst soll das Szenario mit einer realistischen bestmöglichen Entwicklung dargestellt werden. Das Tableau aus Abbildung 7-9 wird dafür erweitert um folgende Größen:

q_{max}	siehe Beschreibung in Abschnitt 7.2.2.2
η_S	siehe Beschreibung in Abschnitt 7.2.2.2
$N_{O,Z}$	siehe Beschreibung in Abschnitt 7.2.2.2
$N_{O,G}$	Anzahl der insgesamt durch den Originalhersteller pro Jahr verkauften Bauteile nach Einführung eines Sicherheitsmerkmals
$U_{O,Z}$	siehe Beschreibung in Abschnitt 7.2.2.2

I	Invest des Originalherstellers zur Erzeugung von Sicherheitsmerkmalen und zur Einrichtung eines Gesamtsystems (kann über die Perioden fortgeschrieben werden, falls Folgeinvestitionen erwartet werden)
k_{var}	Preis für ein einzelnes Sicherheitsmerkmal
K_{var}	stückzahlabhängige variable Kosten zur Ausrüstung der Originalbauteile mit Sicherheitsmerkmalen

Dabei wird das bisherige Beispiel fortgeschrieben mit folgenden Werten:

- q_{max} = 30 %
- η_S wird hier als Mittel verwendet, den situationsbezogenen Wirkungsgrad des Sicherheitsmerkmals über die Jahre zu entwickeln. Analog zu einer typischen Anlaufkurve bei Neueinführung eines Produktes wird hier davon ausgegangen, dass sich dieser Wirkungsgrad über die Perioden positiv entwickelt bis zu einem technologieabhängigen Maximalwert von 70 %. Die Anlaufkurve ist geschätzt, aber der typischen Kurve des Produktlebenszyklus nachempfunden [Bro-13d].
- I = 20.000 € in t = 0 als Anfangsinvest des Originalherstellers zur Erzeugung von Sicherheitsmerkmalen und zur Einrichtung eines Gesamtsystems (dieser Betrag wurde mit Hilfe eines Anbieters ermittelt und fällt relativ gering aus, da im vorliegenden Beispiel aufgrund des Einsatzes von Hologrammen keine technische Prüfinfrastruktur benötigt wurde)
- k_{var} = 0,1 € als Preis für ein einzelnes Sicherheitsmerkmal (dieser Betrag wurde mit Hilfe eines Anbieters ermittelt und bezieht sich auf den Einsatz von Hologrammen)

Szenario Best-Case										
t		0	1	2	3	4	5	6	7	8
N_G	[Stück/Jahr]	154.000	154.000	154.000	154.000	154.000	154.000	154.000	154.000	
N_O	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
N_K	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
q_{max}	[%]	30%	30%	30%	30%	30%	30%	30%	30%	
η_S	[%]	0%	10%	30%	60%	70%	70%	70%	70%	
$N_{O,Z}$	[Stück/Jahr]	0	2.310	6.930	13.860	16.170	16.170	16.170	16.170	
$N_{O,G}$	[Stück/Jahr]	77.000	79.310	83.930	90.860	93.170	93.170	93.170	93.170	
N_K	[Stück/Jahr]	77.000	74.690	70.070	63.140	60.830	60.830	60.830	60.830	
U_G	[Tsd. €]	4.620	4.620	4.620	4.620	4.620	4.620	4.620	4.620	
U_O	[Tsd. €]	2.310	2.310	2.310	2.310	2.310	2.310	2.310	2.310	
$U_{O,Z}$	[Tsd. €]	0	69	208	416	485	485	485	485	
$U_{O,verl}$	[Tsd. €]	-2.310	-2.241	-2.102	-1.894	-1.825	-1.825	-1.825	-1.825	
I	[Tsd. €]	-20								
K_{var}	[Tsd. €]	-8	-8	-8	-9	-9	-9	-9	-9	
$G_{O,verl}$	[Tsd. €]	-1.552	-1.487	-1.396	-1.259	-1.214	-1.214	-1.214	-1.214	
$CF_{statisch}$	[Tsd. €]	-1.552	-1.487	-1.396	-1.259	-1.214	-1.214	-1.214	-1.214	
$CF_{Barwert}$	[Tsd. €]	-1.552	-1.403	-1.242	-1.057	-961	-907	-856	-807	-2.538

K_0 (ohne R_0)	[Tsd. €]	-8.786
R_0	[Tsd. €]	-2.538
$S_{0,gesamt}$	[Tsd. €]	-11.323

Abbildung 7-10: Weiterführung des Beispiels aus Abbildung 7-9, in Anlehnung an [Fuc-09, Gün-13a]

In Abbildung 7-10 sind neben den bisher angegebenen die folgenden Formeln für die jeweilige Periode t angewendet bzw. logisch weiterentwickelt:

$$N_{O,Z}(t) = q_{max}(t) * \eta_S(t) * N_G(t) \quad (7\text{-}15)$$

$$N_{O,G}(t) = N_O(t) + N_{O,Z}(t) \quad (7\text{-}16)$$

$$N_K(t) = N_G(t) - N_{O,G}(t) \quad (7\text{-}17)$$

$$U_{O,Z}(t) = p * N_{O,Z}(t) \quad (7\text{-}18)$$

$$U_{O,verl}(t) = U_G(t) - U_O(t) - U_{O,Z}(t) \quad (7\text{-}19)$$

$$K_{var}(t) = (-1) * k_{var}(t) * N_{O,G}(t) \quad (7\text{-}20)$$

$$G_{O,verl}(t) = g * U_{O,erl}(t) + I_0(t) + K_{var}(t) \quad (7\text{-}21)$$

Vergleicht man das Ergebnis für $S_{0,gesamt}$ im Best-Case (11,3 Mio € in Abbildung 7-10) mit dem Ergebnis für $S_{0,gesamt}$ im Ist-Zustand (13,2 Mio € in Abbildung 7-9) ist erkennbar, dass eine klare Reduktion des Schadens durch Produkt- und Markenpira-

terie bei dem betroffenen Unternehmen im Bezug auf das betrachtete Bauteil zu erwarten wäre. Dies wird insbesondere beim Vergleich der Zeitreihen für die $CF_{Barwert}$ erkennbar (siehe Abbildung 7-11). Dafür werden folgende Größen verwendet:

$CF_{Barwert, Diff}$ Differenz des Gegenwartswerts der jährlichen Cash-Flow-Verluste $CF_{Barwert}$ der verglichenen Szenarien

$K_{0,S}$ Kapitalwert der Investition in ein Sicherheitsmerkmal und Gesamtsystem aufgrund der Verringerung der Schäden durch Produkt- und Markenpiraterie

Bewertung des "Szenario Best-Case"										
$CF_{Barwert,Diff}$	[Tsd. €]	-28	36	115	223	246	232	219	207	650

K_0 (ohne R_0)	[Tsd. €]	1.250
R_0	[Tsd. €]	650
$K_{0,S}$	[Tsd. €]	1.900

Abbildung 7-11: Weiterführung des Beispiels mit dem Vergleich der $CF_{Barwert}(t)$ des Ist-Zustands aus Abbildung 7-9 und der $CF_{Barwert}(t)$ des Best-Case-Szenarios aus Abbildung 7-10, in Anlehnung an [Gün-13a]

Im vorliegenden Fall kann aus dem Vergleich des Ist-Zustands (siehe Abbildung 7-9) sowie dem Best-Case-Szenario (siehe Abbildung 7-10) abgeleitet werden, dass die Reduktion des Schadens aufgrund der Einführung von Sicherheitsmerkmalen sich in einem positiven Kapitalwert der Investition in die Sicherheitsmerkmale in Höhe von 1,9 Mio € ausdrückt. Zudem würde sich diese Investition innerhalb von einer Periode bereits amortisiert haben. Diese sehr positive Sicht soll im Folgenden mit der Betrachtung zweier weiterer Szenarien relativiert werden.

Worst-Case-Szenario

Im Gegensatz zum Best-Case-Szenario wird in diesem Abschnitt davon ausgegangen, dass die Einführung von Sicherheitsmerkmalen lediglich einen minimalen Erfolg bezüglich der Eindämmung der Produkt- und Markenpiraterie bringt. Dies ist im Parameter η_S abgebildet, der in Abbildung 7-12 einen gegenüber Abbildung 7-10 stark gedämpften Verlauf über die Perioden annimmt und sein Maximum bei 7 % erreicht.

Szenario Worst-Case										
t		0	1	2	3	4	5	6	7	8
N_G	[Stück/Jahr]	154.000	154.000	154.000	154.000	154.000	154.000	154.000	154.000	
N_O	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
N_K	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
q_{max}	[%]	30%	30%	30%	30%	30%	30%	30%	30%	
η_S	[%]	0%	3%	5%	7%	7%	7%	7%	7%	
$N_{O,Z}$	[Stück/Jahr]	0	693	1.155	1.617	1.617	1.617	1.617	1.617	
$N_{O,G}$	[Stück/Jahr]	77.000	77.693	78.155	78.617	78.617	78.617	78.617	78.617	
N_K	[Stück/Jahr]	77.000	76.307	75.845	75.383	75.383	75.383	75.383	75.383	
U_G	[Tsd. €]	4.620	4.620	4.620	4.620	4.620	4.620	4.620	4.620	
U_O	[Tsd. €]	2.310	2.310	2.310	2.310	2.310	2.310	2.310	2.310	
$U_{O,Z}$	[Tsd. €]	0	21	35	49	49	49	49	49	
$U_{O,verl}$	[Tsd. €]	-2.310	-2.289	-2.275	-2.261	-2.261	-2.261	-2.261	-2.261	
I	[Tsd. €]	-20								
K_{var}	[Tsd. €]	-8	-8	-8	-8	-8	-8	-8	-8	
$G_{O,verl}$	[Tsd. €]	-1.552	-1.519	-1.510	-1.500	-1.500	-1.500	-1.500	-1.500	
$CF_{statisch}$	[Tsd. €]	-1.552	-1.519	-1.510	-1.500	-1.500	-1.500	-1.500	-1.500	
$CF_{Barwert}$	[Tsd. €]	-1.552	-1.433	-1.343	-1.260	-1.188	-1.121	-1.058	-998	-3.137

K_0 (ohne R_0)	[Tsd. €]	-9.954
R_0	[Tsd. €]	-3.137
$S_{0,gesamt}$	[Tsd. €]	-13.091

Abbildung 7-12: Weiterführung des Beispiels aus Abbildung 7-9 und Abbildung 7-10 [nach Gün-13a sowie in Anlehnung an Fuc-09]

Vergleicht man das Ergebnis des Schadens $S_{0,gesamt}$ im Worst-Case (13,1 Mio € in Abbildung 7-12) mit dem Ergebnis für $S_{0,gesamt}$ im Ist-Zustand (13,2 Mio € in Abbildung 7-9) ist feststellbar, dass $S_{0,gesamt}$ nicht wesentlich verändert ist. Die Differenz der beiden Schadenssummen aus Produkt- und Markenpiraterie beträgt lediglich 132.373 €. Dies wird beim Vergleich der Zeitreihen für die $CF_{Barwert}$ genau erkennbar (siehe Abbildung 7-13).

Bewertung des "Szenario Worst-Case"										
$CF_{Barwert,Diff}$	[Tsd. €]	-28	6	13	20	19	18	17	16	51

K_0 (ohne R_0)	[Tsd. €]	82
R_0	[Tsd. €]	51
$K_{0,S}$	[Tsd. €]	132

Abbildung 7-13: Weiterführung des Beispiels mit dem Vergleich der $CF_{Barwert}(t)$ des Ist-Zustands aus Abbildung 7-9 und der $CF_{Barwert}(t)$ des Worst-Case-Szenarios aus Abbildung 7-12, in Anlehnung an [Gün-13a]

Im vorliegenden Fall kann somit aus dem Vergleich des Ist-Zustands (siehe Abbildung 7-9) mit dem Worst-Case-Szenario (siehe Abbildung 7-13) abgeleitet werden, dass die Reduktion des Schadens aufgrund der Einführung von Sicherheitsmerkma-

len sich in einem positiven Kapitalwert der Investition in die Sicherheitsmerkmale in Höhe von ca. 130.000 € ausdrückt. Die Amortisation ist nach ca. 2,6 Jahren erreicht. Obwohl dies die negative Sicht auf die Gesamtmaßnahme darstellt und die Wirkung als sehr schwach eingeschätzt wurde, kann der Invest in Sicherheitsmerkmale als wirtschaftlich eingestuft werden. Im Folgenden erfolgt noch die Darstellung des wahrscheinlichsten Szenarios.

Trend-Szenario

Im Trend-Szenario wird die wahrscheinlichste Entwicklung abgebildet. Es wird davon ausgegangen, dass dieses Szenario zwischen dem Best- und dem Worst-Case-Szenario liegt. Dies ist erneut im Parameter η_S abgebildet, der in Abbildung 7-14 einen gegenüber Abbildung 7-10 und Abbildung 7-12 moderat positiven Verlauf über die Perioden annimmt und sein Maximum bei 35 % erreicht. Erneut ist darin die im Produktlebenszyklus typische Anlaufkurve für neue Produkte nachempfunden [Bro-13d].

Szenario Trend										
t		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
N_G	[Stück/Jahr]	154.000	154.000	154.000	154.000	154.000	154.000	154.000	154.000	
N_O	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
N_K	[Stück/Jahr]	77.000	77.000	77.000	77.000	77.000	77.000	77.000	77.000	
q_{max}	[%]	30%	30%	30%	30%	30%	30%	30%	30%	
η_S	[%]	0%	5%	15%	30%	35%	35%	35%	35%	
$N_{O,Z}$	[Stück/Jahr]	0	1.155	3.465	6.930	8.085	8.085	8.085	8.085	
$N_{O,G}$	[Stück/Jahr]	77.000	78.155	80.465	83.930	85.085	85.085	85.085	85.085	
N_K	[Stück/Jahr]	77.000	75.845	73.535	70.070	68.915	68.915	68.915	68.915	
U_G	[Tsd. €]	4.620	4.620	4.620	4.620	4.620	4.620	4.620	4.620	
U_O	[Tsd. €]	2.310	2.310	2.310	2.310	2.310	2.310	2.310	2.310	
$U_{O,Z}$	[Tsd. €]	0	35	104	208	243	243	243	243	
$U_{O,verl}$	[Tsd. €]	-2.310	-2.275	-2.206	-2.102	-2.067	-2.067	-2.067	-2.067	
I	[Tsd. €]	-20								
K_{var}	[Tsd. €]	-8	-8	-8	-8	-9	-9	-9	-9	
$G_{O,verl}$	[Tsd. €]	-1.552	-1.510	-1.464	-1.396	-1.373	-1.373	-1.373	-1.373	
$CF_{statisch}$	[Tsd. €]	-1.552	-1.510	-1.464	-1.396	-1.373	-1.373	-1.373	-1.373	
$CF_{Barwert}$	[Tsd. €]	-1.552	-1.424	-1.303	-1.172	-1.088	-1.026	-968	-913	-2.871

K_0 (ohne R_0)	[Tsd. €]	-9.446
R_0	[Tsd. €]	-2.871
$S_{0,gesamt}$	[Tsd. €]	-12.317

Abbildung 7-14: Weiterführung des Beispiels aus Abbildung 7-9, Abbildung 7-10 und Abbildung 7-12, in Anlehnung an [Fuc-09, Gün-13a]

Die Bewertung der Veränderung des Schadens $S_{0,gesamt}$ in Höhe von 12,3 Mio € (siehe Abbildung 7-14) erfolgt erneut in Bezug auf $S_{0,gesamt}$ aus dem Ist-Zustand in Höhe

von 13,2 Mio € (siehe Abbildung 7-9) und dem Verlgeich der Zeitreihen für die $CF_{Barwert}$ (siehe Abbildung 7-15).

Bewertung des "Szenario Trend"										
$CF_{Barwert,Diff}$	[Tsd. €]	-28	14	54	108	120	113	107	101	317

K_0 (ohne R_0)	[Tsd. €]	590
R_0	[Tsd. €]	317
$K_{0,S}$	[Tsd. €]	906

Abbildung 7-15: Weiterführung des Beispiels mit dem Vergleich der $CF_{Barwert}(t)$ des Ist-Zustands aus Abbildung 7-9 und der $CF_{Barwert}(t)$ des Trend-Szenarios aus Abbildung 7-14, nach [Gün-13a]

Somit kann abgeleitet werden, dass sich im vorliegenden Beispiel die Reduktion des Schadens aufgrund der Einführung von Sicherheitsmerkmalen in einem positiven Kapitalwert der Investition in die Sicherheitsmerkmale $K_{0,S}$ in Höhe von ca. 906.000 € ausdrückt. Die Amortisation ist nach ca. 1,75 Jahren erreicht (siehe Abbildung 7-15).

Zusammenfassung und Interpretation

Für das Beispiel wurden vier Zustände bzw. Szenarien abgebildet (siehe Abschnitt 7.2.2.3):

- Ist-Zustand
- Best-Case-Szenario
- Worst-Case-Szenario
- Trend-Szenario

Dabei wurden jeweils diese wesentlichen Größen bestimmt:

- $S_{0,gesamt}$
- $K_{0,S}$

Für eine sinnfällige Visualisierung empfiehlt es sich, die passenden Größen im zeitlichen Verlauf darzustellen (siehe Abbildung 7-16 und Abbildung 7-17). Dabei zeigt sich, dass die Verläufe für die Szenarien klar gestaffelt sind.

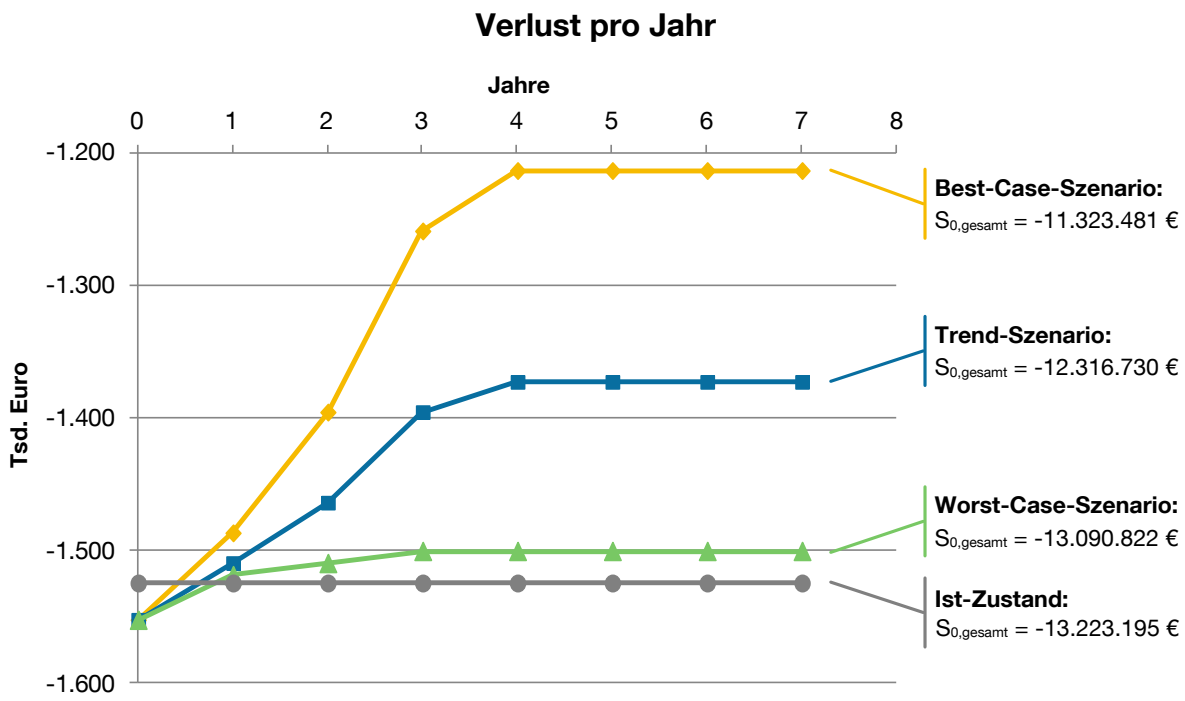


Abbildung 7-16: Zeitlicher Verlauf der Verluste pro Jahr für den Ist-Zustand und die drei Szenarien [24]

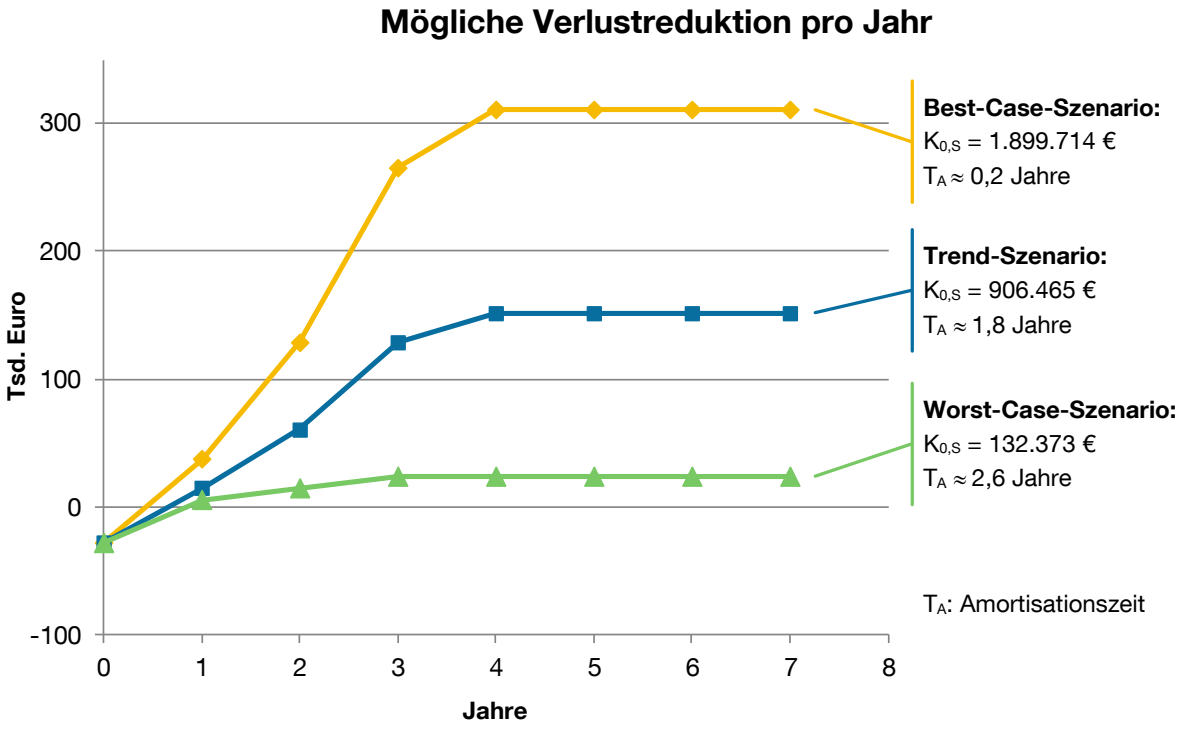


Abbildung 7-17: Zeitlicher Verlauf der Reduktion der Verluste pro Jahr für die drei Szenarien gegenüber dem Ist-Zustand [25]

[24] Abbildung der zeitlichen Verläufe der CFstatisch aus Abbildung 7-9, Abbildung 7-10, Abbildung 7-12 und Abbildung 7-14

Insbesondere liegen alle Szenarien mit $K_{0,S}$ im positiven Bereich, so dass im vorliegenden Beispiel auch im Worst-Case kein Verlust aus dieser Maßnahme zu erwarten ist. Daher empfiehlt es sich in diesem Beispiel, die angedachte Maßnahme umzusetzen.

Um die Szenarien weiter zu verfeinern ist es möglich, weitere Parameter im zeitlichen Verlauf zu variieren und Ereignisse mit Auswirkungen auf die Marktsituation zu berücksichtigen, um so die zeitlichen Verläufe immer mehr der möglichen zukünftigen Realität anzunähern:

- Steigende Werte für N_G aufgrund eines prognostizierten Marktwachstums
- Zeitlicher Verlauf für p aufgrund erwarteter Preisentwicklung
- Veränderung von N_K aufgrund eines erwarteten gerichtlichen Verbots für Produktion und Vertrieb von Kopien eines unredlichen Wettbewerbers in einer bestimmten Periode
- etc.

Natürlich können in anderen Fällen die Werte für $K_{0,S}$ in allen Szenarien negativ ausfallen, weil beispielsweise der Invest im Jahr t=0 und etwaige Nachfolgeinvestitionen in den darauffolgenden Perioden den Gewinn aus dem zusätzlich zu erwartenden Umsatz aufzehren. Das vorliegende Beispiel kann somit nicht verallgemeinert werden. Es dient vielmehr dazu, ein methodisches Vorgehen vorzuschlagen und aufzuzeigen, um den Schaden durch Produkt- und Markenpiraterie im Ist-Zustand herzuleiten und die Wirkung etwaiger Maßnahmen wie die Kennzeichnung und Authentifizierung von Originalbauteilen monetär bewertbar zu machen.

Wildemann hat zur wirtschaftlichen Bewertung und Auswahl von passenden Sicherheitsmerkmalen ein weiteres Verfahren entwickelt. Dieses stellt die abgeschätzten Kosten aus dem Invest des Originalherstellers zur Erzeugung von Sicherheitsmerkmalen und zur Einrichtung eines Gesamtsystems zu deren Überprüfung gegenüber dem Invest, den der Originalhersteller bereit wäre, in diese Maßnahme zu investieren. Ein zeitlicher Verlauf der Kosten und der Wirkung, wie das in der vorliegenden Arbeit entwickelte Verfahren dies erlaubt, ist damit nicht abzuleiten. [veröffentlicht in Gün-11a, Wil-11]

[25] Abbildung der zeitlichen Verläufe der Differenz der $CF_{statisch}$ aus Abbildung 7-10, Abbildung 7-12, Abbildung 7-14 im Bezug auf Abbildung 7-9

7.2.3 Beispiele als Ergebnis der Auswahl passender Sicherheitsmerkmale auf Basis wirtschaftlicher Auswahlkriterien

Die in den Abschnitten 5.2.2 und 7.1.3 abgebildeten Beispiele (S. 89 und 121) werden hier fortgesetzt. Nach der Bestimmung der technisch passenden Sicherheitsmerkmale erfolgt für die ausgewählten schützenswerten Bauteile eine wirtschaftliche Bewertung. So wird die je schützenswertem Bauteil optimal passende Sicherheitstechnologie bestimmt. Die detaillierte Darstellung dieser Inhalte darf nicht veröffentlicht werden. Die Ergebnisse dieses Prozesses sind jedoch in Abbildung 7-18 dargestellt.

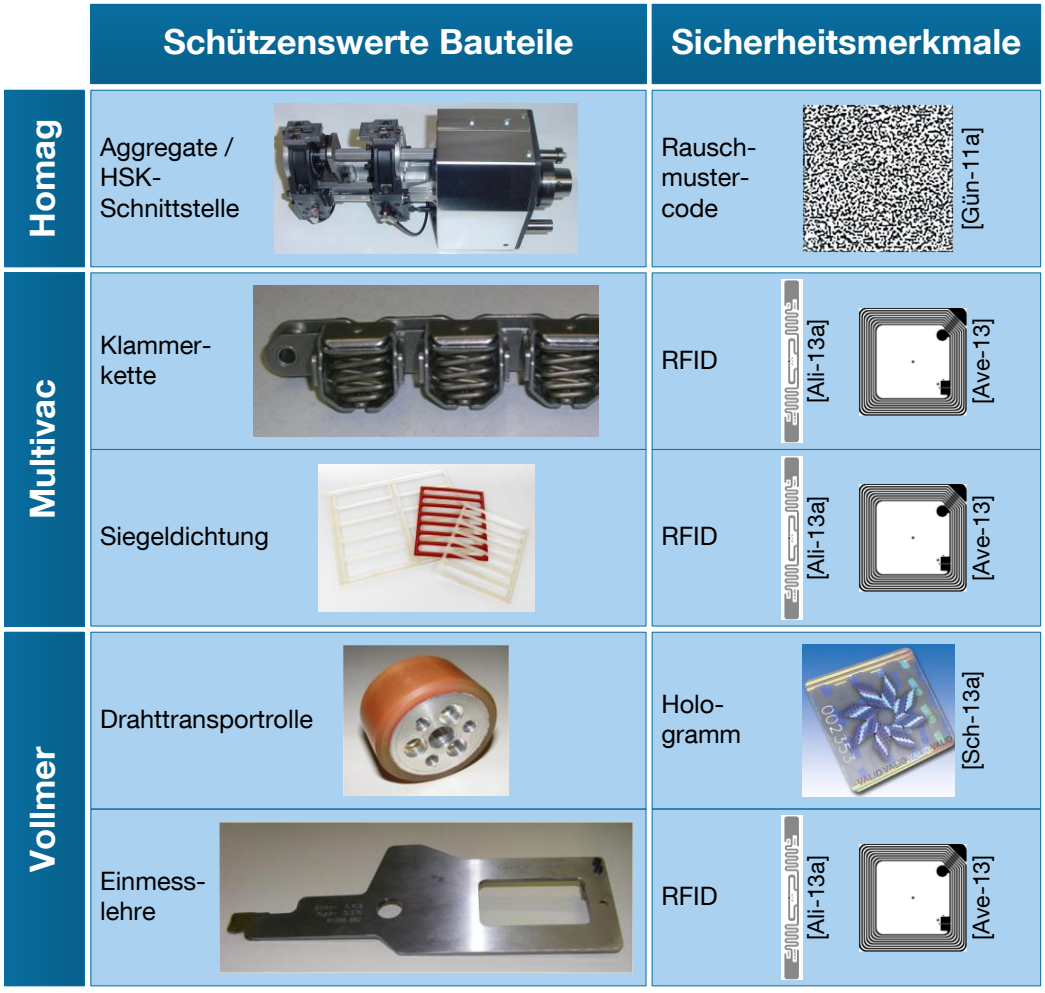


Abbildung 7-18: **Beispiele schützenswerter Bauteile und der mittels wirtschaftlicher Auswahlkriterien bestimmter Sicherheitstechnologien (Bildquellen Bauteile: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, Vollmer Werke Maschinenfabrik GmbH)**

7.3 Unikatkennzeichen als Kombination von Originalitäts- und Identitätskennzeichen

Neben den in Anhang A aufgeführten und in Anhang D eingestuften Unikatkennzeichen gibt es eine weitere, sehr verbreitete Möglichkeit, ein Unikatkennzeichen zu erzeugen: die Kombination eines Originalitätskennzeichens mit einem Identitätskennzeichen (siehe Abschnitt 2.7.1, S. 27). Ein Identitätskennzeichen kann ein 1D-Barcode, ein 2D-Barcode, ein RFID-Transponder oder ähnliches sein (siehe Abbildung 3-3, S. 45). Dabei besteht der große Vorteil der Identitätskennzeichen darin, dass diese (meist) maschinenlesbar und somit automatisiert erfassbar sind. Die Kombination mit einem Originalitätskennzeichen bringt dann zusätzlich die Sicherheit des Fälschungsschutzes.

Um nun für ein bestimmtes schützenswertes Bauteil ein passendes Kennzeichen als Kombination aus Identitäts- und Originalitätskennzeichen zu entwickeln, sollte zunächst festgestellt werden, welches Identitätskennzeichen ausgewählt werden soll. Dies ist oftmals schon festgelegt, da die in den Unternehmen bereits verwendeten Systeme auch im Falle der Einführung eines technischen Produktpiraterie-Schutzsystems genutzt werden können oder sollen. Danach kann mit den in den Abschnitten 7.1 und 7.2 bereits vorgestellten Verfahren das passende Originalitätskennzeichen ausgewählt werden, indem die Anforderungen an dieses Kennzeichen geschickt gewählt werden.

Die Anforderungen an das Gesamtkennzeichen, also die Kombination aus Identitäts- und Originalitätskennzeichen, können aufgeteilt werden in Anforderungen, welche das Identitätskennzeichen betreffen, sowie Anforderungen, welche durch das Originalitätskennzeichen erfüllt werden müssen. Die Anforderungen an das Gesamtkennzeichen, welche bereits durch das Identitätskennzeichen abgedeckt werden, können dann zusätzlich, müssen aber nicht zwingend auch vom Sicherheitsmerkmal erfüllt werden. Sind diese Anforderungen an das Sicherheitsmerkmal bestimmt, führt die in den Abschnitten 7.1 und 7.2 dargestellte Methode zur sicheren Auswahl eines für das schützenswerte Bauteil passenden Sicherheitsmerkmals.

Nach Festlegung des Identitätskennzeichens sowie des Sicherheitsmerkmals kann in Zusammenarbeit mit den Unternehmen, welche Sicherheitsmerkale anbieten, eine Gesamtlösung für die Applikation des Gesamtkennzeichens sowie dessen Authentifizierung erarbeitet werden. Ein mögliches Ergebnis dieses Vorgehens könnte aus-

sehen wie die von der Deutschen Post AG verwendete Paketmarke (Abbildung 7-19).

Abbildung 7-19: Unikatkennzeichen als Kombination aus Identitätskennzeichen und Originalitätskennzeichen (Bildquelle Paketmarke: [Deu-13d], Bildquelle Hologramm: eigene Aufnahme)

Die Möglichkeit der Kombination von Identitätsmerkmalen mit Originalitätskennzeichen ist insbesondere deshalb interessant, weil bestehende T&T-Systeme durch diese neue Funktionalität ergänzt werden könnten. Sicher ist dafür auch die technische Ausstattung der I-Punkte zu IP-Punkten notwendig. Dies kann aber sukzessive erfolgen. In einem T&T-System werden sehr häufig die in Abbildung 7-20 angegebenen Identitätskennzeichen verwendet.

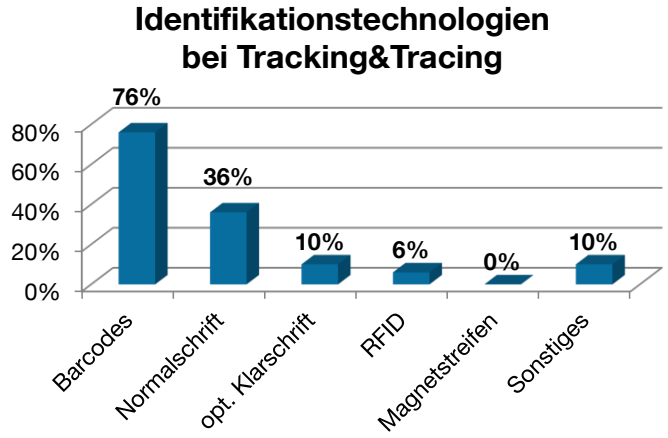


Abbildung 7-20: Identitätskennzeichen in existierenden T&T-Systemen, Mehrfachnennungen möglich [Bre-02 S. 17]

7.4 RFID als Sicherheitsmerkmal

Radiofrequenzidentifikation (RFID, siehe Abbildung 7-21) ist eine Technologie, die es erlaubt, „Objekte und Personen eindeutig, schnell, berührungslos, gleichzeitig und ohne direkte Sichtverbindung zu identifizieren. Durch den Einsatz von RFID-Systemen können demnach Objekte (nahezu) gleichzeitig erfasst werden. Das heißt, befinden sich mehrere Objekte mit je einem RFID-Transponder im Feld vor einer RFID-Antenne, so können diese bequem in einem Vorgang identifiziert werden.“ [fml-13c]

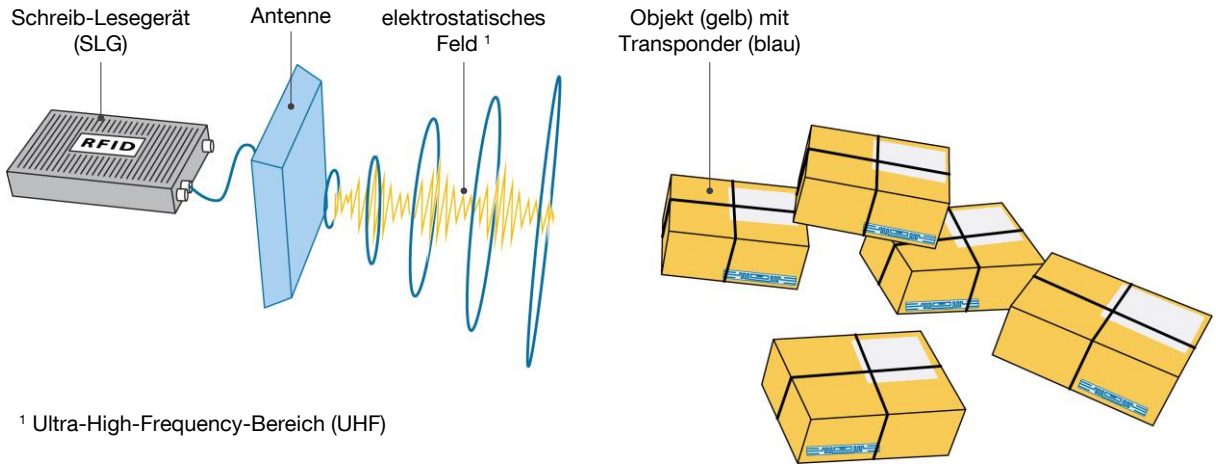


Abbildung 7-21: Grundlegende Bestandteile eines RFID-Systems (Bildquelle: [fml-13c], Bezeichnungen: [Fin-12 S. 63 f.])

Aus dieser Definition ist abzuleiten, dass RFID zunächst nur zur Identifizierung von Objekten und nicht zur Authentifizierung genutzt werden kann (vergleiche hierzu die Definitionen in Abschnitt 2.7.1, S. 27). Dies bedeutet, dass RFID zunächst keine Technologie darstellt, welche als Sicherheitsmerkmal dienen kann. Dennoch gilt unter den verfügbaren Technologien RFID als Favorit zum Schutz von Originalen vor Produkt- und Markenpiraterie [Fuc-06 S. 275, Ste-09]. Dies liegt daran, dass ein RFID-Transponder auf verschiedenen Wegen technisch ausgestattet oder eingesetzt werden kann, um diesen als Sicherheitsmerkmal zu verwenden. Daher ist diese Technologie auch in den Anhängen A und D aufgenommen.

In den folgenden Abschnitten soll nach einem Einblick in den Aufbau und die Funktionsweise eines RFID-Transponders ein Überblick über die Möglichkeiten gegeben werden, wie RFID als Sicherheitsmerkmal eingesetzt werden kann.

7.4.1 RFID-Transponder: Speicheraufbau und Datenmodell

Hier soll am Beispiel eines RFID-Systems im Ultra-High-Frequency-Bereich (UHF) gezeigt werden, wie ein Transponder-System aufgebaut ist und als Unikatkennzeichen im Kampf gegen Produktpiraterie eingesetzt werden kann. Dieses System arbeitet mit einer Feldfrequenz zwischen 860 MHz und 960 MHz und wird häufig in der Logistik eingesetzt [Bar-08 S. 26, 39, 94, 153, Kov-12, Wei-12].

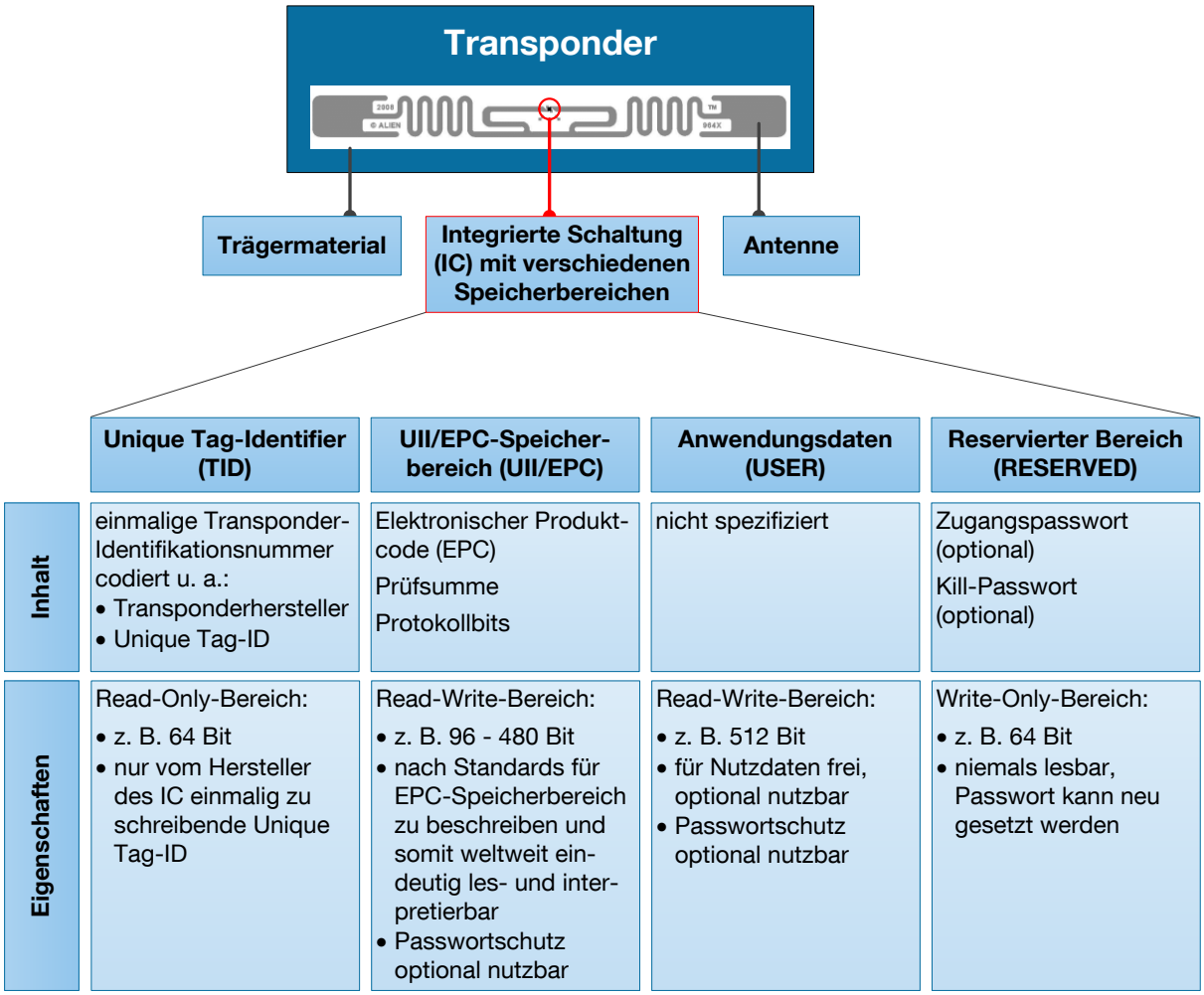
In diesem UHF-Frequenzbereich gibt es den sogenannten „Gen-2-Standard“, der eine sehr große Marktattraktivität hat und in zwei gespiegelten Standards beschrieben wird: einerseits in der Norm der Internationalen Organisation für Normung (ISO) „ISO/IEC 18000-63:2013“, andererseits im Standard der weltweit operierenden, offenen Non-Profit-Organisation EPCglobal Inc. „EPC™ RFID Radio-Frequency Identity Protocols. Class-1 Generation-2 UHF RFID. Protocol for Communications at 860 - 960 MHz” [ISO18000-63, EPC-08, siehe auch Fin-12 S. 365, S. 378 ff.].

Ein RFID-Transponder besteht aus einer Integrierten Schaltung (IC) und einer Antenne auf einem Trägermaterial [fml-13d]. Im IC sind dabei, wie in Abbildung 7-22 zu sehen, nach Gen-2-Standard vier verschiedene Speicherbereiche angelegt [ISO18000-63 S. 30, EPC-08 S. 37]:

- Unique Tag-Identifier (TID):
  Der Unique Tag-Identifier (TID) ist eine weltweit überschneidungsfreie Identifikationsnummer, die vom Transponderhersteller derart in den Speicher des Transponder-ICs geschrieben wird, dass diese nicht veränderbar ist. Darin sind die Registrierungsnummer des Transponderherstellers sowie eine von ihm vergebene Seriennummer enthalten. [ISO15963]
- UII/EPC-Speicherbereich (UII / EPC):
  Der Speicherbereich für den Unique Item Identifier (UII, nach ISO) bzw. den Electronic Product Code (EPC, nach EPCglobal) dient dazu, ein Objekt oder eine Ware eindeutig identifizieren zu können. Dabei werden im UII / EPC das Unternehmen, welches das Produkt herstellt, und auch die von diesem Unternehmen vergebene Sachnummer repräsentiert. Um ein Objekt oder eine Ware zusätzlich weltweit zu individualisieren und damit einmalig zu machen, kann eine Seriennummer vergeben und mitcodiert werden [EPC-08, ISO15459-1, ISO15459-2, ISO15459-3, ISO15459-4, ISO15459-5, ISO15459-6, ISO15459-8, ISO18000-63, Kov-12 S. 60]. So ist sichergestellt, dass dieser

Code und damit das jeweilige Objekt weltweit nur einmal existiert und identifizierbar ist.

- Anwendungsdaten (USER):
  Der User-Bereich kann beispielsweise für weitere produkt- oder auch herstellungsspezifische Daten genutzt werden [ISO18000-63 S. 38, EPC-08 S. 43]. Prinzipiell kann dafür jedes Format verwendet werden. Sollen die abgelegten Daten jedoch von weiteren Wirtschaftsbeteiligten gelesen werden können, sollten diese entsprechend der Norm der ISO/IEC 15962 [siehe ISO15962] oder dem EPCglobal Tag Data Standards [siehe GS1-13b] codiert werden.
- Reservierter Bereich (RESERVED):
  In diesem Speicherbereich können zwei Passwörter angelegt werden: das Access-Passwort als Schreib- und Leseschutz für Inhalte der Read-Write-Bereiche und das Kill-Passwort, um bei Wunsch den Transponder permanent zu deaktivieren [ISO18000-63 S. 31, EPC-08 S. 38, Sky-13].



	Unique Tag-Identifier (TID)	UII/EPC-Speicher-bereich (UII/EPC)	Anwendungsdaten (USER)	Reservierter Bereich (RESERVED)
Inhalt	einmalige Transponder-Identifikationsnummer codiert u. a.: • Transponderhersteller • Unique Tag-ID	Elektronischer Produkt-code (EPC) Prüfsumme Protokollbits	nicht spezifiziert	Zugangspasswort (optional) Kill-Passwort (optional)
Eigenschaften	Read-Only-Bereich: • z. B. 64 Bit • nur vom Hersteller des IC einmalig zu schreibende Unique Tag-ID	Read-Write-Bereich: • z. B. 96 - 480 Bit • nach Standards für EPC-Speicherbereich zu beschreiben und somit weltweit ein-deutig les- und inter-pretierbar • Passwortschutz optional nutzbar	Read-Write-Bereich: • z. B. 512 Bit • für Nutzdaten frei, optional nutzbar • Passwortschutz optional nutzbar	Write-Only-Bereich: • z. B. 64 Bit • niemals lesbar, Passwort kann neu gesetzt werden

Abbildung 7-22: RFID-UHF-Transponder mit seinen verschiedenen Bestandteilen sowie dem Aufbau des Speicherbereichs, nach [EPC-08, GS1-13b, ISO18000-63] (Quelle Transponder & technische Daten: [Ali-13b], Bestandteile des Transponders: in Anlehnung an [fml-13d])

Sobald ein Objekt mit einem RFID-Transponder versehen ist, kann dessen UII/EPC-Speicherbereich mit einem UII nach ISO oder auch einem EPC nach EPCglobal beschrieben werden. Damit ist der Transponder und gleichzeitig auch das Objekt weltweit eindeutig identifizier- und wiedererkennbar, sofern der Nummerngeber auch eine Seriennummer vergibt. Dabei folgen der Aufbau des UII oder auch des EPC demselben Schema (siehe Abbildung 7-23).

UII/EPC-Speicherbereich (UII/EPC)			
Prüf-, Steuer-, Attribute-Bits	**Identifikationsnummer des Nummerngebers**	**Objektnummer**	**Seriennummer (optional)**
z. B. Unterscheidung UII oder EPC	„EPCglobal Manager“ oder „Company Identification Number (CIN)“ meist des Herstellers der Ware	z. B. Artikelnummer als Zuordnung zur Artikelklasse, vergeben durch den Nummerngeber	z. B. Seriennummer zur Individualisierung des einzelnen Objekts, vergeben durch den Nummerngeber

Abbildung 7-23: Aufbauschema des UII bzw. EPC [Fin-12, GS1-13b, ISO15459-1 bis -6, Kov-12, Oeh-10]

7.4.2 Authentifizierung mittels UII / EPC und TID auf Basis eines Datenbankabgleichs

Sobald ein Objekt mit Hilfe eines Transponders und eines serialisierten UII / EPC versehen und somit weltweit einmalig ist, kann dieses Objekt sehr einfach authentifiziert werden. Dafür ist im Gesamtsystem zur dokumentierten Authentifizierung von schützenswerten Bauteilen im Maschinen- und Anlagenbau eine Datenarchivierung und -auswertung notwendig (siehe Abbildung 5-2, S. 86). In dieser legt der Originalhersteller bei der Kennzeichnung des Originalbauteils in der Produktion einen initialen Datensatz für dieses Bauteil an. Dieser Datensatz muss in jedem Fall den UII / EPC des Bauteils enthalten, umfasst aber sinnvollerweise auch weitere Daten (siehe Abschnitt 8.2, S. 181).

Bei jeder Identifikation an einem IP-Punkt, die auch eine Wareneingangs- oder -ausgangsbuchung bei einem der Beteiligten in der originalen Wertschöpfungs- und Logistikkette verursachen kann, kann gleichzeitig die Authentifizierung der Waren erfolgen. Der gelesene UII / EPC wird dafür über eine Datenverbindung an das Datenarchivierungs- und -auswertesystem gesendet (siehe Abbildung 7-24). Dort erfolgt eine einfache Prüfung durch einen Datenabgleich: „Wurde ein Datensatz vom Hersteller angelegt, der diesen UII / EPC enthält?“, mit zwei möglichen Ausgängen:

- „Ja“, dann ist das vorliegende Objekt ein Original.
- „Nein“, dann kann das vorliegende Objekt nicht als Original bestätigt werden.

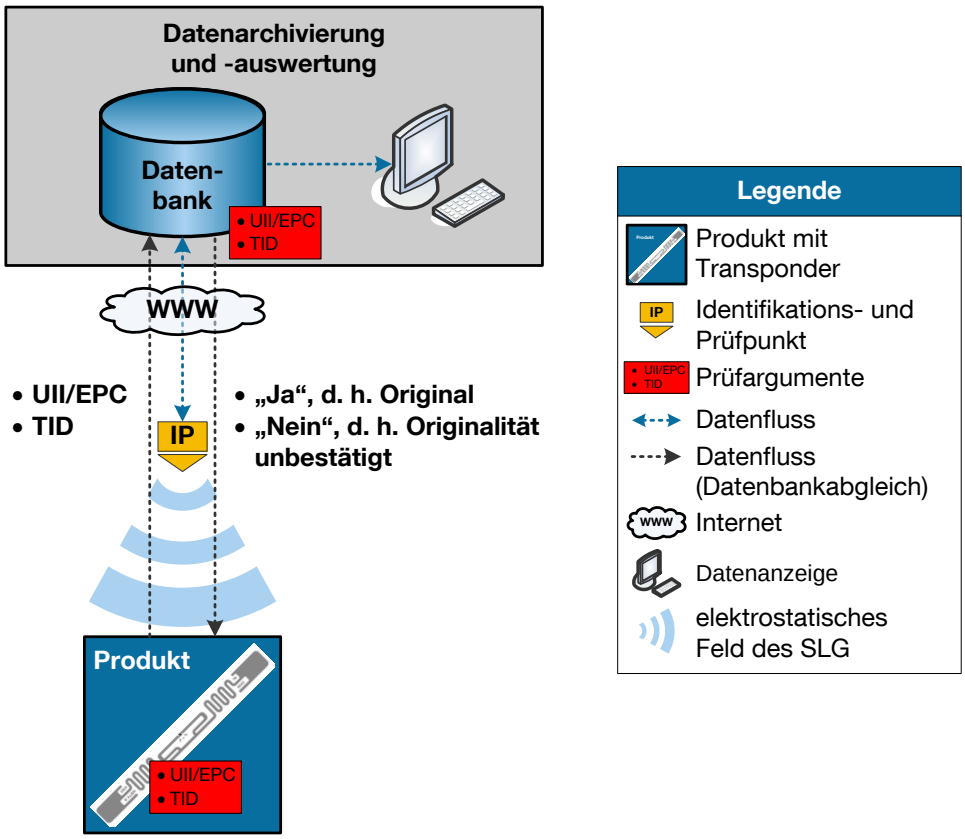


Abbildung 7-24: Authentifizierung mittels Datenbankabgleich

Das Ergebnis der Prüfung wird an den IP-Punkt zurückübermittelt zur Anzeige für einen Mitarbeiter oder zur Generierung einer automatischen Systemreaktion (z. B. Ausschleusen des Objektes für weitere Prüfungen). Problematisch bei der Nutzung des UII / EPC in der beschriebenen Form ist, dass sich der UII / EPC in einem Read-Write-Bereich des Transponders befindet und somit zwei Gefahren existieren:

1. Gefahr der Veränderung des UII / EPC:
   Der UII / EPC könnte durch einen Beteiligten der Logistikkette versehentlich oder absichtlich verändert werden mit der Konsequenz, dass das vorliegende Bauteil nicht mehr als Original authentifiziert werden kann.
2. Gefahr durch Kopieren des UII / EPC:
   Da der UII / EPC durch jeden Wirtschaftsbeteiligten weltweit gelesen werden können soll, könnte ein unredlicher Wettbewerber diesen auslesen und kopieren. Eine Kopie des Originalbauteils könnte somit mit einem Transponder mit demselben UII / EPC ausgestattet werden wie das Original und somit an IP-Punkten auch als Original bestätigt werden.

Um dem ersten Fall zu begegnen, kann der für Gen-2-Transponder vorgesehene Passwortschutz genutzt werden. Durch das Einrichten eines Passworts kann der

UII/EPC-Speicherbereich gegen Überschreiben geschützt werden [siehe EPC-08 S. 38, GS1-13b S. 133, ISO18000-63 S. 30].

Damit ist aber der schwerwiegendere zweite Fall noch nicht gelöst. Um den zweiten Fall zu verhindern, könnte im Datenarchivierungs- und -auswertesystem parallel zur Authentifizierung ein Plausibilitätscheck durchgeführt werden. Dieser würde bei einer Anfrage überprüfen, ob das betreffende Objekt an diesem Ort sein kann oder soll. Dabei könnte ein Abgleich mit Lieferavisen stattfinden oder mit Ort-Zeit-Beziehungen insofern gearbeitet werden, als klar ist, dass ein Objekt nicht an zwei Orten gleichzeitig sein kann oder eine gewisse Zeit für die Ortsveränderung benötigt. Eine sicherere Möglichkeit ist, dass – entweder zusätzlich zum UII / EPC oder auch alleine – die weltweit einmalige TID für den Datenbankabgleich genutzt wird. Die TID wird vom IC-Hersteller in den Read-Only-Bereich des Transponders geschrieben und kann somit zwar gelesen, aber niemals in den für die TID vorgesehenen Speicherbereich geschrieben werden.

Die Authentifizierung eines Transponders und damit des Objektes, an dem dieser befestigt ist, mit Hilfe der TID und einem Datenbankabgleich ist somit eine der einfachsten Möglichkeiten, die Originalität eines Transponders festzustellen.

Der Nachteil bei diesem Verfahren ist, dass eine Datenbankverbindung bestehen muss. Zudem besteht die Möglichkeit, einen Transponder zu emulieren, d. h. identisch nachzuahmen [Bro-13e]. Dieser Aufwand ist jedoch insofern hoch, dass ein unredlicher Wettbewerber ein RFID-Schreib-Lesegerät (RFID-SLG) und eine Antenne derart aufbauen müsste, dass dieses SLG dieselben Daten an das anfragende SLG des IP-Punktes zurückgibt, wie dies der Original-Transponder tun würde. Dabei könnte mit diesem Aufbau lediglich ein einziger Originaltransponder (und nicht alle Originaltransponder) nachgeahmt werden, dessen Daten bekannt sind. Der Schaden am Gesamtsystem wäre also relativ gering. Eine Emulation eines Originaltransponders kann jedoch mit Challenge-Response-Verfahren verhindert werden.

7.4.3 Challenge-Response und Krypto-Transponder

Mit Challenge-Response-Verfahren kann ein höheres Sicherheitsniveau erreicht werden, denn ein Challenge-Response-Verfahren sieht vor, dass dem zu prüfenden Transponder eine Aufgabe in Form einer „Challenge“ übermittelt wird. Diese Challenge muss vom Transponder korrekt verarbeitet und es muss eine „Response“ als Antwort zurückgegeben werden. Ist die Response korrekt, handelt es sich um einen

Originaltransponder. Im anderen Fall kann die Originalität nicht bestätigt werden. [Rot-05, Wil-07 S. 92f.]

Im Bereich der Challenge-Response-Verfahren gibt es verschiedene Möglichkeiten – hier werden das symmetrische und das asymmetrische Verfahren vorgestellt.

7.4.3.1 Challenge-Response: Symmetrisches Verfahren

Bei einem symmetrischen Challenge-Response-Verfahren wird dem Transponder eine Challenge übermittelt, die dieser Transponder mit dem ihm bekannten Schlüssel bearbeitet und die so berechnete Response an das SLG sendet (siehe Abbildung 7-25). Das SLG übergibt die Response an die fragende Einheit (im einfachsten Fall ein Computer, in komplexeren Systemen eine zentrale Entität zur Datenarchivierung und -auswertung). Da der fragenden Einheit derselbe Schlüssel bekannt ist, kann diese ebenfalls die Response berechnen. Bei Gleichheit beider Response-Aussagen ist der Transponder und damit das Produkt ein Original [Rot-05, Swo-08 S. 152, Wil-07 S. 92f.]

Da die Challenge bei jeder Anfrage anders ist, verändert auch die passende Response sich ständig. Ein Abhören der Datenübertragung mit dem Ziel der Emulation des Transponders ist nicht möglich [Fin-12 S. 248, Rot-05, Swo-08 S. 152]. Sollte jedoch der Schlüssel zur Erzeugung der zu einer Challenge passenden Response außerhalb des Systems bekannt werden, ist das gesamte System unsicher [Rot-05].

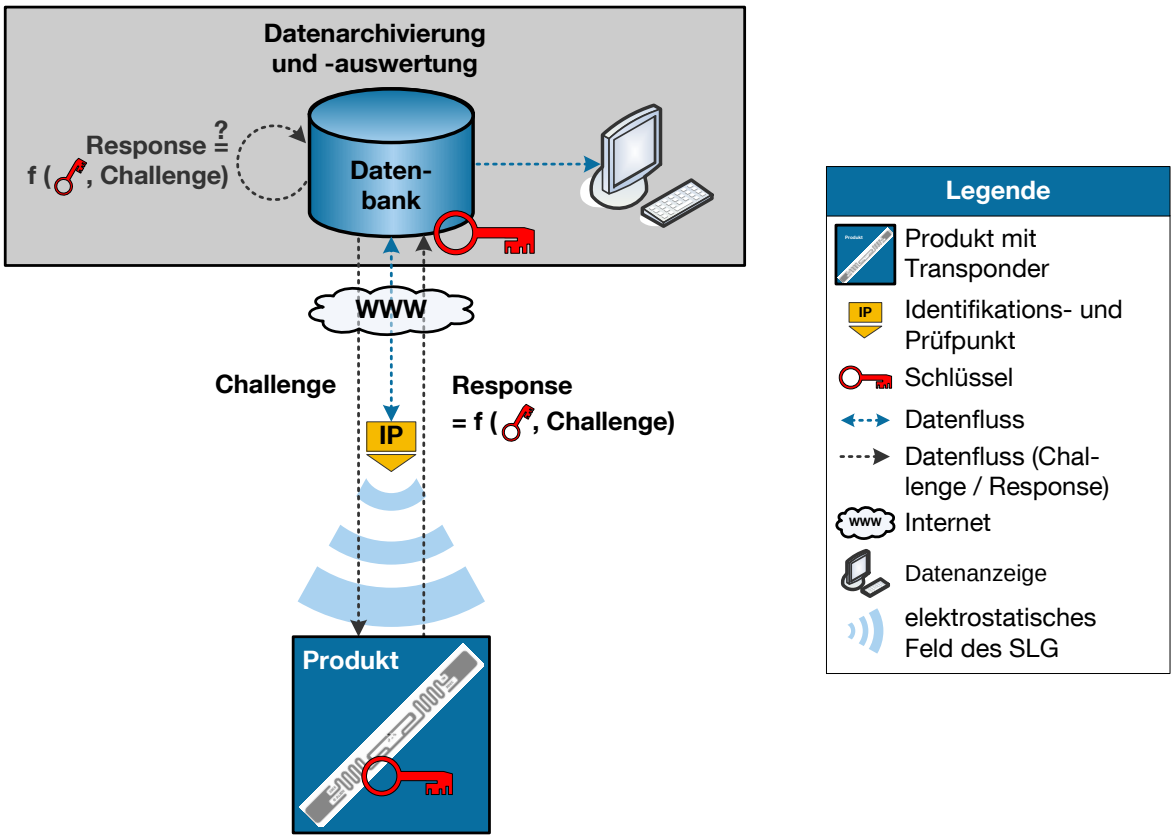


Abbildung 7-25: Symmetrisches Challenge-Response-Verfahren, inhaltlich in Anlehnung an [Swo-08 S. 152]

7.4.3.2 Challenge-Response: Asymmetrisches Verfahren

Das asymmetrische Challenge-Response-Verfahren arbeitet mit einem Schlüsselpaar. Dieses Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel. Der private Schlüssel wird dabei im Transponder zur Berechnung der Response auf entsprechende Challenge-Anfragen abgelegt und kann nicht von einem Transponder auf einen anderen übertragen werden. Der öffentliche Schlüssel hingegen wird öffentlich kommuniziert, da dieser zur Prüfung der Response-Angabe dient (siehe Abbildung 7-26). Bei Verwendung dieses asymmetrischen Verfahrens kann der IP-Punkt nach Erhalt des öffentlichen Schlüssels auch offline arbeiten und die Authentifizierung durchführen. [Bra-08b, ITP-13, Sie-13b, Ste-09]

Die mit kryptografischen Funktionen ausgestatteten Transponder liegen aufgrund der komplexeren Struktur preislich etwas höher als vergleichbare Transponder ohne dieses Sicherheitsfeature.

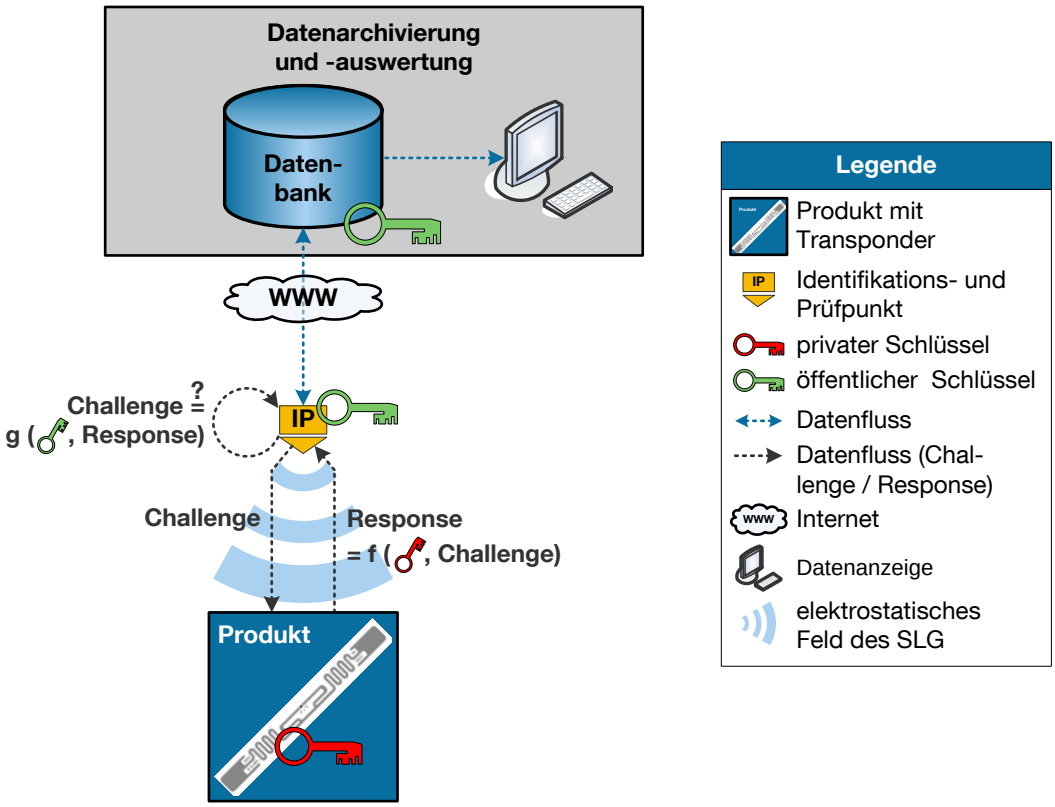


Abbildung 7-26: Asymmetrisches Challenge-Response-Verfahren, inhaltlich in Anlehnung an [Swo-08 S. 153, Ste-09]

7.4.4 Digitale Signatur

Mit Hilfe von digitalen Signaturen ist es möglich, die sehr preiswerten Gen-2-Transponder (siehe Abschnitt 7.4.1) ebenfalls auf ein sehr hohes Sicherheitsniveau zu heben und somit als Sicherheitsmerkmal für Originalprodukte einzusetzen.[26] Dabei können Verfahren der Authentifizierung mit digitalen Signaturen zur Anwendung kommen.

Die Funktionsweise der Authentifizierung eines Transponders und damit der Prüfung der Originalität eines Produkts, an dem dieser Transponder befestigt oder integriert ist, ist in Abbildung 7-27 dargestellt. Zur Erzeugung einer digitalen Signatur verschlüsselt der Originalhersteller Inhalte der Speicherbereiche des Transponders – idealerweise die weltweit einmalige TID aus dem Read-Only-Speicher und den weltweit einmaligen UII / EPC aus dem Read-Write-Bereich.

[26] „Sicherheit“ ist ein Begriff, der quantitativ nicht zu bewerten ist [ITP-13]. Daher sind die einzelnen Systeme auch nicht echt vergleichbar oder in einem Ranking abzubilden.

Dafür erfolgt zunächst an einem speziell ausgestatteten IP-Punkt in der Produktion des Originalherstellers eine Anfrage an den Transponder, um die TID und den UII / EPC zu erhalten. Zur Erzeugung der digitalen Signatur aus diesen beiden Argumenten verwendet der Originalhersteller seinen privaten Schlüssel eines asymmetrischen kryptografischen Verfahrens [Eck-08 S. 317 f., Sch-06, Swo-08 S. 153]. Dieser private Schlüssel ist Teil eines Schlüsselpaares, dessen zweiter Teil ein öffentlicher Schlüssel darstellt, und muss geheim gehalten werden. So ist sichergestellt, dass allein der Originalhersteller in der Lage ist, eine korrekte Signatur zu erzeugen. Mit Hilfe des SLG schreibt der Originalhersteller die erzeugte Signatur in den freien USER-Speicherbereich des Transponders. Der vollständig beschriebene Transponder ist dabei nach den in Abschnitt 5.4.1, S. 96 formulierten Anforderungen als Sicherheitsmerkmal mit dem Produkt manipulationssicher verbunden (siehe auch Abschnitt 7.5).

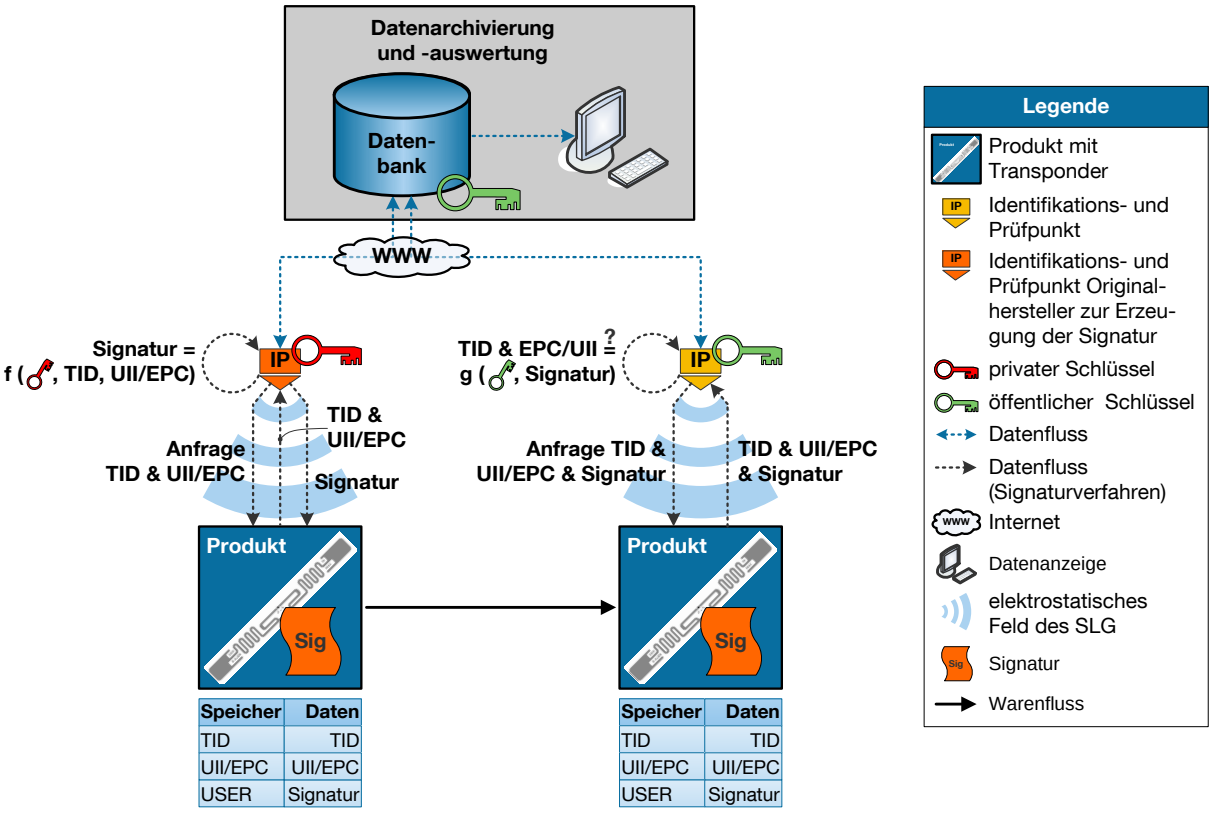


Abbildung 7-27: Authentifizierung mittels digitaler Signatur, inhaltlich in Anlehnung an die Vorveröffentlichungen des Autors in [Ben-10, Gün-11c S. 23], siehe auch [Dur-12, Gri-08]

Um das Produkt mittels des an- / eingebrachten Transponders zu authentifizieren, werden an einem IP-Punkt innerhalb des Wertschöpfungs- und Logistiknetzwerks alle drei Speicherbereiche ausgelesen: TID, UII / EPC und USER-Speicherbereich mit der digitalen Signatur. Mit Hilfe eines öffentlichen Schlüssels, den der Original-

hersteller zur Verfügung stellt, wird die digitale Signatur entschlüsselt. Daraus ergeben sich dann wieder die beiden Argumente TID und der UII / EPC. Sind die Ergebnisse der Entschlüsselung identisch mit der TID und der UII / EPC, die in Klartext aus den Speicherbereichen gelesen wurden, handelt es sich bei dem vorliegenden Produkt um ein Original. Ansonsten kann die Originalität nicht bestätigt werden.

Auch eine Manipulation am Transponder würde entdeckt werden. Der UII / EPC befindet sich im Read-Write-Speicherbereich des Transponders und könnte prinzipiell verändert werden – aus Versehen oder absichtlich. Bei der Entschlüsselung der Signatur wäre dann der entschlüsselte UII / EPC ungleich dem Speicherinhalt des UII/EPC-Speicherbereichs. Jedoch die TID, die im Read-Only-Bereich steht, wäre weiterhin identisch mit der entschlüsselten TID aus der Signatur. Somit kann die Originalitätsprüfung drei Ergebnisse erzeugen:

- UII / EPC (Speicherbereich) = UII / EPC (aus Signatur) und
  TID (Speicherbereich) = TID (aus Signatur) bedeutet:
  Produkt ist ein Original und die UII/EPC-Daten wurden nicht verändert.
- UII / EPC (Speicherbereich) ≠ UII / EPC (aus Signatur) und
  TID (Speicherbereich) ≠ TID (aus Signatur) bedeutet:
  Das Produkt ist kein Original.
- UII / EPC (Speicherbereich) ≠ UII / EPC (aus Signatur) und
  TID (Speicherbereich) = TID (aus Signatur) bedeutet:
  Das Produkt ist ein Original, aber die UII/EPC-Daten wurden verändert.

Welche kryptografischen Verfahren für die Erzeugung einer digitalen Signatur verwendet werden können, wird im nächsten Abschnitt dargestellt.

7.4.5 Kryptografische Verfahren

Kryptografische Verfahren werden seitens ISO bereits seit 1990 beschrieben [siehe ISO9798-1, ISO9798-2]. Zudem sind diese Verfahren als Algorithmen in öffentlichen Bibliotheken verfügbar, beispielsweise im „MSDN: das Microsoft Developer Network“ [MSDN-13a].

Für das Verfahren der Authentifizierung mit digitalen Signaturen (siehe Abschnitt 7.4.4) kommen folgende kryptografische Verfahren in Frage, die zur Zeit allgemein als die sichersten betrachtet werden und zur Anwendung empfohlen werden [Bun-13c S. 6, Bar-12 S. 38 f.]:

- RSA: Rivest, Shamir, Adleman (benannt nach den Erfindern des Algorithmus)
- DSA: Digital Signature Algorithm
- ECDSA: DSA auf Elliptischen Kurven

Insbesondere die Algorithmen DSA und ECDSA sind dabei zu empfehlen. Denn bei einer Signaturlänge von 448 Bit hat der DSA und der ECDSA eine IT-technisch / mathematische Sicherheit bis zum Jahr 2015. Bei einer Signaturlänge von 512 Bit sind diese beiden Algorithmen bis 2019 als sicher einzustufen [Bun-13c S. 8, Bar-12 S. 37].

Die entstehende Signaturlänge ist im Falle von RFID mit entscheidend, da auf den Transpondern im USER-Speicherbereich nur eingeschränkter Speicherplatz zur Verfügung steht. Die in Tabelle 7-9 angegebenen Schlüssellängen wären ideal, denn der USER-Speicher hat bei gängigen Gen-2-Transpondern eine Größe von 512 Bit [siehe beispielsweise Ali-13b].

Tabelle 7-9: Vergleich der Signatur- und Schlüssellängen kryptografischer Verfahren, die bis Ende 2015 als sicher eingestuft werden, in Anlehnung an [Bun-13c S. 8, Bar-12 S. 37]

Algorithmus	Länge der Signatur [Bit]	Länge des privaten Schlüssels [Bit]	Länge des öffentlichen Schlüssels [Bit]
RSA	2048	2048	2048
DSA	448	224	2048
ECDSA	448	224	2048

7.5 Auf- / Einbringen des Sicherheitsmerkmals auf / in schützenswerte Bauteile und Komponenten

Nach der Auswahl des Sicherheitsmerkmals für das jeweilige schützenswerte Bauteil erfolgt die Planung für das physische Auf- / Einbringen des Kennzeichens auf / in das Bauteil. Dafür gibt es verschiedene Möglichkeiten: vom manuellen Applizieren über teilautomatische Lösungen bis hin zur vollautomatischen Applikation im Herstellungsprozess des schützenswerten Bauteils.

Die technische Realisierung kann also sehr unterschiedlich sein und ist abhängig von dem Bauteil selbst und dessen Material oder Substrat, dem Herstellungsprozess des Bauteils, dem verwendeten Sicherheitsmerkmal, der Anzahl an zu markie-

renden Originalbauteilen, etc. Daher muss dieser Prozess individuell gestaltet werden. Dabei ist insbesondere die Expertise der Sicherheitsmerkmale anbietenden Unternehmen gefragt, um eine möglichst kostenoptimale Lösung zu generieren. Was hier allgemeingültig angegeben werden kann, ist ein Überblick über die Möglichkeiten der Verbindungen zwischen Merkmal und Produkt sowie Eckpunkte für eine optimale Lösung des Markierungsprozesses.

7.5.1 Möglichkeiten der Verbindungen zwischen Merkmal und Produkt und Eckpunkte für eine optimale Lösung des Markierungsprozesses

Zur Applikation eines Sicherheitsmerkmals auf / in einem Originalprodukt sind in Tabelle D-1, S. D-1 in der Spalte „Verbindung Merkmal – Produkt“ abhängig der Technologie folgende Möglichkeiten angegeben:

- EI: Einbringen in das Produkt
- OS: Nutzung der vorhandenen Oberflächenstruktur am Produkt
- OÄ: Oberflächenänderung am Produkt
- OA: Oberflächenauftrag auf das Produkt
- ET: Verwendung eines Etiketts

Die Reihenfolge ist dabei bewusst gewählt, denn die optimale Lösung stellt sicherlich das Einbringen eines Merkmals in ein Produkt dar, gefolgt von den weiteren Möglichkeiten. Die reine Verwendung der unveränderten Oberfläche oder einer zielgerichtet veränderten Oberfläche wiederum ist einem reinen Oberflächenauftrag vorzuziehen. Die Verwendung eines Etiketts ist zwar die einfachste Möglichkeit, aber auch diejenige, die am ehesten nachzuahmen oder abhängig vom gewählten Sicherheitsmerkmal sogar kopierbar ist.

Neben der Form dieser Verbindung sollten bei der Gestaltung des Markierungsprozesses auch die Forderungen aus Abschnitt „5.4.1 Anforderungen an Sicherheitsmerkmale“ sowie die Angaben zur Belastbarkeit der Authentifizierung in Abschnitt „7.1.2.3 Vorbereitungen für Feinplanung und Ausgestaltung“ berücksichtigt werden. Diese ergeben zusammen folgende Eckpunkte für den optimalen Markierungsprozess, also das optimale Auf- / Einbringen des Sicherheitsmerkmals auf / in ein schützenswertes Bauteil:

- Das Auf- / Einbringen sollte während der Produktion des Originalbauteils stattfinden, so dass das Sicherheitsmerkmal möglichst integraler Bestandteil

des schützenswerten Bauteils ist. So kann sichergestellt werden, dass das Sicherheitsmerkmal nicht nachträglich anbringbar und somit eine sehr hohe Fälschungssicherheit gewährleistet ist.

- Die Verbindung zwischen Sicherheitsmerkmal und Originalbauteil sollte so gestaltet sein, dass das Merkmal während des gesamten Produktlebenszyklus vorhanden und nicht (spurenfrei) entfernbar oder übertragbar auf andere Produkte ist. So ist eine dauerhafte Authentifizierbarkeit des Originalprodukts möglich. Hierbei ist das Einbringen in das Produkt sicherlich die beste Wahl.
- Um sicherzustellen, dass ein auf oder in das Originalbauteil auf- oder eingebrachte Sicherheitsmerkmal auch im Extremfall bei gerichtlichen Auseinandersetzungen Bestand hat, muss der Markierungsprozess zusätzlich zwei Bedingungen erfüllen: Der Markierungsprozess für Originalwaren muss so ausgestaltet sein, dass nachweisbar sichergestellt ist, dass jedes Originalprodukt, welches veräußert wird, ein Sicherheitsmerkmal trägt. Zudem muss sichergestellt sein, dass keine Blanko-Sicherheitsmerkmale das Unternehmen verlassen können – die Sicherheitsmerkmale müssen somit unter Verschluss gehalten und beispielsweise abgezählt zur Markierung einer bestimmten Menge von Originalbauteilen ausgegeben werden. Das Sicherheitsmerkmal selbst darf darüber hinaus weltweit nicht zufällig mehrfach existieren.

Je früher im Produktlebenszyklus der Markierungsprozess etabliert wird, desto einfacher ist dessen Integration in den Herstellprozess eines Bauteils und desto größer ist die Wahrscheinlichkeit, dass sich die Investition amortisiert.

Schützenswerte Bauteile können Bauteile sein, die bereits im Einsatz sind und bei welchen der Herstellungsprozess bereits festgelegt ist. Andererseits können es aber auch Bauteile sein, die sich noch in der Entwicklungsphase und somit in ihrem Produktlebenszyklus vor dem Markteintritt befinden. Hier gibt es natürlich größere Gestaltungsfreiheiten hinsichtlich des Markierungsprozesses als es bei bereits existierenden Bauteilen der Fall ist. Daher sollte möglichst früh festgestellt werden, ob in einem Unternehmen ein Bauteil als schützenswert einzustufen ist oder nicht, um etwaige Sicherheitsmerkmale sowie deren Applikation bereits in der Entwicklungsphase zu berücksichtigen.

7.5.2 Beispiele für die Verbindung zwischen Merkmal und schützenswertem Bauteil

Die in den Abschnitten 5.2.2, 7.1.3 und 7.2.3 abgebildeten Beispiele (S. 89, 121 und 157) werden hier fortgesetzt. Nach der Bestimmung der passenden Sicherheitsmerkmale erfolgte für die gewählten schützenswerten Bauteile das Auf- oder Einbringen der Sicherheitsmerkmale mit dem in Abbildung 7-28 dargestellten Ergebnis.

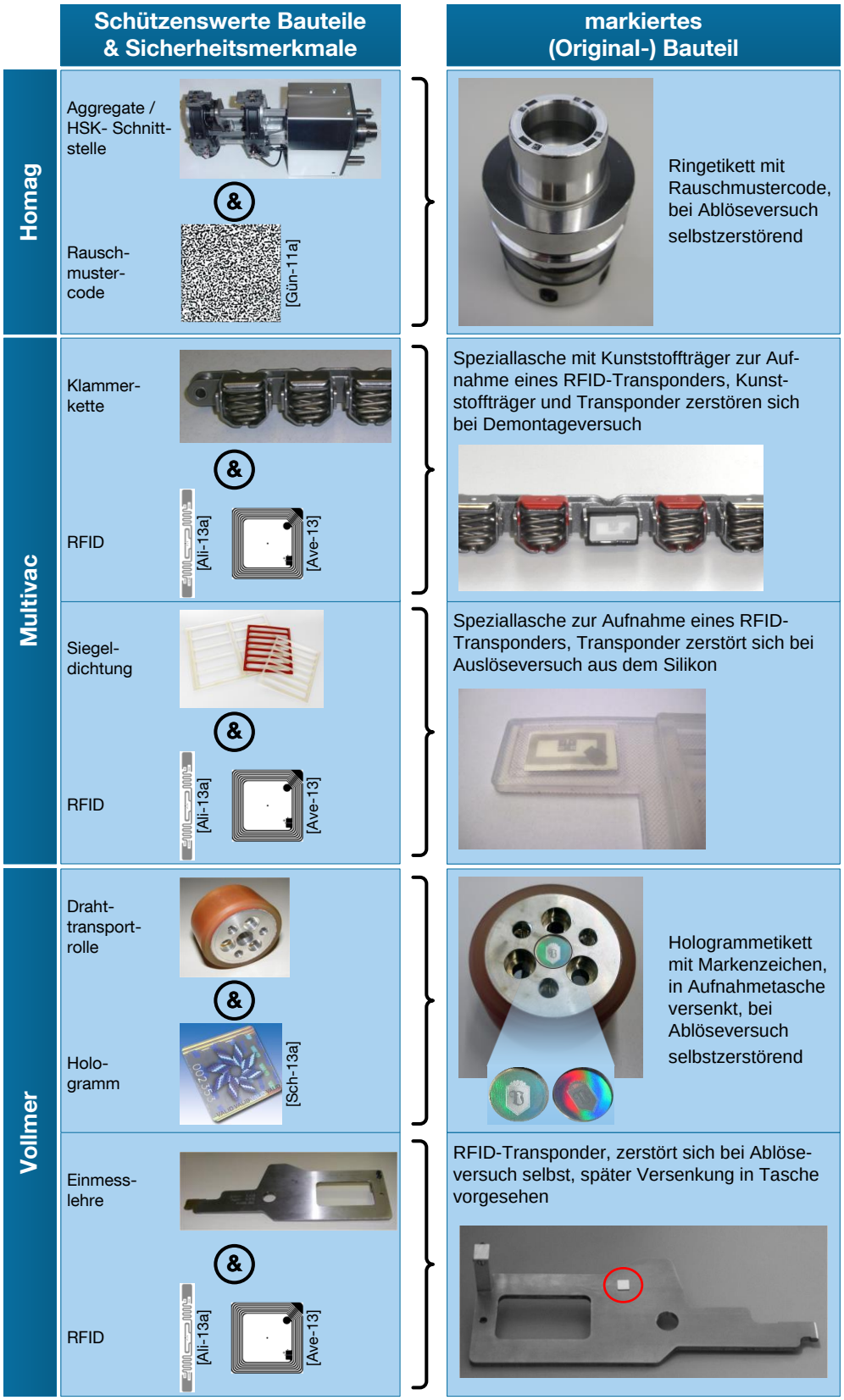


Abbildung 7-28: Beispiele schützenswerter Bauteile mit auf- / eingebrachten Sicherheitsmerkmalen (Bildquellen Bauteile: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, Vollmer Werke Maschinenfabrik GmbH)

7.6 Zusammenfassung und Abgleich der Ergebnisse mit den Anforderungen an das Sicherheitsmerkmal

In den Abschnitten 7.1 bis 7.5 wurde ein methodisches Vorgehen entwickelt, mit dem für ein schützenswertes Bauteil ein oder mehrere passende Sicherheitsmerkale bestimmt und anschließend mit einer Wirtschaftlichkeitsbetrachtung bewertet werden können. Zusammen mit den Inhalten der Kapitel 5 und 6 gibt es somit ein methodisches Vorgehen, das beinhaltet bzw. berücksichtigt:

- die Auswahl schützenswerter Bauteile
- das Branding von Originalbauteilen, also die Markierung mit geschützten Markenzeichen
- die Methodik zur Auswahl der passenden Sicherheitsmerkmale für ein schützenswertes Bauteil auf Basis technischer Auswahlkriterien
- die Methodik zur Bewertung der Wirtschaftlichkeit von Sicherheitsmerkmalen inklusive des passenden Gesamtsystems zur Authentifizierung
- die Vorgehensweise zur Generierung eines Unikatkennzeichens als Kombination aus Sicherheitsmerkmalen und Identitätskennzeichen
- Möglichkeiten der Verwendung von RFID als Sicherheitsmerkmal
- Hinweise für einen optimalen Markierungsprozess zum Auf- / Einbringen des Sicherheitsmerkmals auf / in das Originalbauteil

Dass die mittels diesem methodischen Vorgehen bestimmten Sicherheitsmerkmale den in Abschnitt 5.4.1, S. 96 bzw. Tabelle 5-1, S. 99 formulierten Anforderungen genügen, ist in der folgenden Tabelle dargestellt.

Tabelle 7-10: Eigenschaften der in den vorangegangenen Abschnitten beschriebenen Systeme

Nr.		Beschreibung
1		**Anforderungen an Sicherheitsmerkmale**
	1.1 ✓	**Eindeutigkeit:** Die in Anhang A aufgeführten und in Anhang D charakterisierten Sicherheitsmerkmale genügen dieser Anforderung, denn die Unternehmen, welche diese Sicherheitsmerkmale anbieten, sind aufs Äußerste bedacht, die Herstellprozesse für die Sicherheitsmerkmale geheim zu halten, sowie dafür Sorge zu tragen, dass keine Sicherheitsmerkmale fälschlicherweise in Umlauf geraten. Dies wird durch entsprechende Prüfungen und Zertifizierungen dieser Unternehmen sichergestellt. Zudem ist in Anhang D die Kopiersicherheit angeführt (siehe Punkt 2), mit Hilfe derer Merkmale ausgewählt werden können, die mit dem heutigen Stand der Technik nicht kopiert werden können.
	1.2 ✓	**Fälschungssicherheit:** Es gibt bei den in Anhang A aufgeführten und in Anhang D charakterisierten Sicherheitsmerkmalen Unterschiede im Aufwand, die ein unredlicher Wettbewerber betreiben müsste, um ein Sicherheitsmerkmal zu fälschen. Dabei reicht die Spannweite von „dieses Merkmal ist mit einfachen Hilfsmitteln nachahmbar“ bis „dieses Merkmal ist mit dem heutigen Stand der Technik nicht fälschbar“. Dies ist abgebildet in Anhang D, Spalte „Kopiersicherheit“. Somit kann ein Unternehmen abhängig des eigenen Sicherheitsbedürfnisses die Auswahl entsprechend treffen.
	1.3 ✓	**Dauerhaftigkeit:** Die Dauerhaftigkeit eines Sicherheitsmerkmals ist gegeben durch die Form der Verbindung zwischen Merkmal und Produkt sowie den Belastungen, denen dieses Produkt während der Einsatzzeit ausgesetzt ist. Die Dauerhaftigkeit kann durch entsprechende Maßnahmen (z. B. Schutzlackierung) signifikant erhöht werden und muss mit den Unternehmen, welche die jeweiligen Sicherheitsmerkmale anbieten, angepasst werden. Daher ist dieser Punkt in Abschnitt „7.1.2.3 Vorbereitungen für Feinplanung und Ausgestaltung“ und "7.5.1 Möglichkeiten der Verbindungen zwischen Merkmal und Produkt und Eckpunkte für eine optimale Lösung des Markierungsprozesses" berücksichtigt.
	1.4 ✓	**Wirtschaftlichkeit:** Zur Überprüfung der Wirtschaftlichkeit des Einsatzes von Sicherheitsmerkmalen kann das in Abschnitt 7.2 abgebildete Vorgehen durchlaufen werden. Die Wirtschaftlichkeit kann somit auf Basis unterschiedlicher Szenarien aufgezeigt werden.

Das entwickelte Vorgehen ermöglicht es einem Unternehmen des Maschinen- und Anlagenbaus, schützenswerte Bauteile zu bestimmen, passende Sicherheitsmerkmale gemäß der formulierten Anforderungen auszuwählen, diese in Zusammenarbeit mit den Unternehmen, welche diese Sicherheitsmerkmale anbieten, zu bewerten und den Markierungsprozess zu gestalten.

In den nachfolgenden Kapiteln wird dargestellt, wie das Gesamtsystem zur dokumentierten Prüfung konzipiert und aufgebaut werden kann, um Originale zu sichern und deren Weg durch das Wertschöpfungsnetzwerk nachvollziehbar festzuhalten. Zudem wird aufgezeigt, welche zusätzlichen Systemfunktionen es ermöglichen, das Gesamtsystem für die Hersteller der Originale sowie deren Kunden und die weiteren Wirtschaftsbeteiligten im Wertschöpfungs- und Logistiknetzwerk attraktiv auszugestalten.

8 Konzeption und Struktur eines IT-Systems für den Produktpirateriesschutz

Die mit Sicherheitsmerkmalen gekennzeichneten schützenswerten Bauteile (siehe Kapitel 7) werden im technischen Produktpiraterie-Schutzsystem authentifiziert und die Prüfergebnisse dokumentiert. Ein dafür passendes System wird in diesem Kapitel konzeptioniert. Dies stellt gleichzeitig „Schritt 4“ des strategischen Vorgehens für Unternehmen dar (siehe Abbildung 5-6, S. 92).

In Abbildung 5-2, S. 86 ist das Referenzszenario für das Produktpiraterie-Schutzsystem dargestellt. Dabei handelt es sich um ein System, das die Ansätze des Produkt- und Markenschutzes sowie des T&T integriert (siehe Abschnitt 1.2.2, S. 8). Visualisiert ist eine am Materialfluss orientierte Anordnung der Beteiligten in der Wertschöpfungs- und Logistikkette sowie die Warenströme zwischen diesen Beteiligten. Zur Errichtung des angestrebten Produktpiraterie-Schutzsystems ist als verbindendes Element ein verteiltes IT-System (siehe Definition) notwendig.

Verteiltes System:
„Ein verteiltes System ist eine Ansammlung unabhängiger Computer, die den Benutzern wie ein einzelnes kohärentes System erscheinen.“ [Tan-08 S. 19, identisch in Dun-08 S. 11]

Dieses verteilte IT-System für den Produktpirateriesschutz baut auf der Systematik von T&T-Systemen auf (siehe Abschnitt 3.2.1, S. 41) und setzt sich aus folgenden Elementen zusammen:

- Logistische Einheiten (siehe Abschnitt 8.1):
  Originalwaren des Originalherstellers mit Unikatkennzeichen bzw. mit integriertem Identitäts- und Originalitätskennzeichen
- IP-Punkte (siehe Abschnitt 8.2):
  Punkte in der Supply-Chain, die analog zu I-Punkten in T&T-Systemen logistische Einheiten identifizieren, diese aber zusätzlich auf Basis der gewählten Sicherheitsmerkmale authentifizieren können

- IT-System zur Datenarchivierung und -auswertung (siehe Abschnitt 8.3):
  System zur Archivierung und Auswertung von T&T-Daten, aber auch der Daten zur Originalität der logistischen Einheiten
- Datenübertragung (siehe Abschnitt 8.3):
  Kommunikation der T&T- / Originalitätsdaten vergleichbar zur Datenübertragung in T&T-Systemen

8.1 Logistische Einheit mit Identitäts- und Sicherheitsmerkmalen

Der Originalhersteller kennzeichnet seine schützenswerten Komponenten und Ersatzteile bei der Herstellung mit Sicherheitsmerkmalen, welche eine eindeutige und permanente Unterscheidung gegenüber etwaigen Kopien von redlichen oder unredlichen Wettbewerbern während des gesamten Produktlebenszyklus erlauben. Gleichzeitig erhalten die Originalbauteile ein Identitätskennzeichen, welches das jeweilige Produkt gegenüber allen weiteren Produkten derselben Sachnummer unterscheidbar macht (siehe Abschnitt 3.2.1.1, S. 44). Damit sind für das jeweilige Produkt auch die T&T-Funktionalitäten nutzbar. Beide Funktionen können in einem Sicherheitsmerkmal als Unikatkennzeichen oder in einer Kombination aus einem Identitätskennzeichen und einem Originalitätskennzeichen repräsentiert sein[27].

Die Auswahl der schützenswerten Bauteile sowie die Auswahl und Integration der passenden Sicherheitsmerkmale ist in Kapitel 7, S. 105 beschrieben. Die Ergebnisse dieses Prozesses sind an Beispielen in Abbildung 7-28, S. 176 zu sehen. Für diese derartig gekennzeichneten Originalprodukte wird hier das in Abbildung 8-1 dargestellte Symbol eingeführt.

Die Drahttransportrolle von Vollmer trägt lediglich ein Originalitäts- und kein Identitätskennzeichen (siehe in Abbildung 7-28, S. 176). Wie Bauteile mit reinen Originalitätskennzeichen innerhalb des Produktpiraterie-Schutzsystem sinnvoll verwendet und authentifiziert werden können, wird in Abschnitt 8.5 dargestellt.

[27] Definitionen siehe 2.7.1, S. 26; Unikatkennzeichen als Kombination von Originalitäts- und Identitätskennzeichen siehe Abschnitt 7.3, S. 158

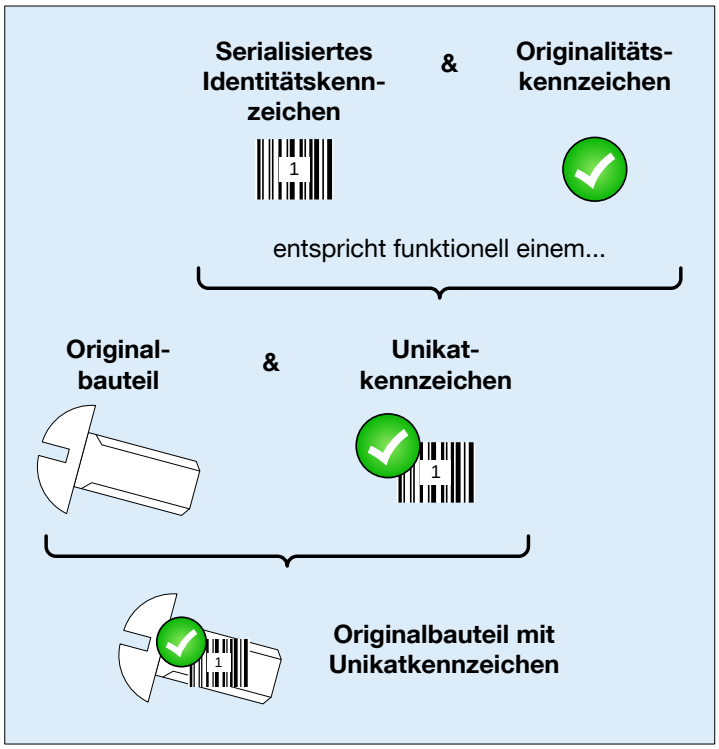


Abbildung 8-1: Symbol für ein Originalbauteil mit Unikatkennzeichen

8.2 Identifikations- und Prüfpunkte zur Authentifizierung und Erzeugung von Prüfdatensätzen

Die gekennzeichneten Originalbauteile können damit jederzeit identifiziert und authentifiziert werden. Dies geschieht analog zu den in Abschnitt 3.2.1, S. 41 beschriebenen I-Punkten. An den im Produktpiraterie-Schutzsystem speziell eingerichteten IP-Punkten ist es damit möglich, die Identität der markierten Originalbauteile und insbesondere auch deren Originalität festzustellen.

Identifikations- und Prüfpunkt (IP-Punkt):
Ein IP-Punkt ist ein Ort in der Supply-Chain, an dem logistische Einheiten mittels elektronisch lesbaren Etiketten identifiziert werden. An diesem Punkt erfolgt gleichzeitig eine Authentifizierung mittels der an den logistischen Einheiten angebrachten Sicherheitsmerkmalen. Die Identiät, etwaige beinhaltete transportrelevante Informationen, Orts- und Zeitangabe sowie das Ergebnis der Authentifizierung (also „Original“ oder „nicht Original“) werden an das zugehörige Datenarchivierungs- und -auswertesystem weitergeleitet.
(Erweiterung der Definition eines I-Punktes aus Abschnitt 3.2.1, S. 41)

Der Aufbau eines IP-Punktes erfolgt dabei analog dem Aufbau eines I-Punktes (siehe Abbildung 3-4, S. 46) und lehnt sich damit an die VDI-Richtlinie 4416 an [VDI4416]. Das Unikatkennzeichen des Originalbauteils wird dabei mit Hilfe der Sende- / Empfangseinrichtung gescannt und das Signal an die Auswerteeinheit übertragen. Die Auswerteeinheit ist ein Rechner in verschiedenen Erscheinungsformen (z. B. Personal Computer (PC), Industrie-PC, Notebook, Steuerung, eingebettetes System).

Bei einer Online-Authentifizierung (siehe Abbildung 8-2) erfolgt die Authentifizierung auf Basis des gelesenen Sicherheitsmerkmals, das die Auswerteeinheit hierfür an die zentrale Datenarchivierung und -auswertung weitergibt. Dort erfolgt der Authentifzierungsschritt mittels des zentral gespeicherten Algorithmus. Wichtig ist, dass das Prüfergebnis der lokalen Auswerteeinheit mitgeteilt und dem Nutzer sofort an der Anzeige des IP-Punktes visualisiert wird. Ein Beispiel für eine Online-Authentifizierung enthält Abbildung 7-24, S. 165 und Abbildung 7-25, S. 168.

Für den Nachweis und ein späteres Nachvollziehen der erfolgten Prüfungen wird bei jedem Prüfvorgang ein Datensatz angelegt und sowohl lokal gespeichert als auch in die zentrale Datenarchivierung übermittelt, sofern die Datensätze dafür freigegeben sind. So können sämtliche Funktionalitäten des T&T genutzt werden und gleichzeitig ist lokal jederzeit die gesamte Prüfhistorie einsehbar, was im Falle von Maschinen und Anlagen besonders wichtig ist. Dieser Vorgang wird in Abschnitt 8.3 vertieft. Der je Prüfvorgang erzeugte Datensatz enthält neben den klassischen Informationen des T&T[28] insbesondere das Ergebnis der Authentifizierung im Argument „Originalität“ (siehe Abbildung 8-3).

[28] siehe Abschnitt 3.2.1, S. 41 mit Abbildung 3-2, S. 44

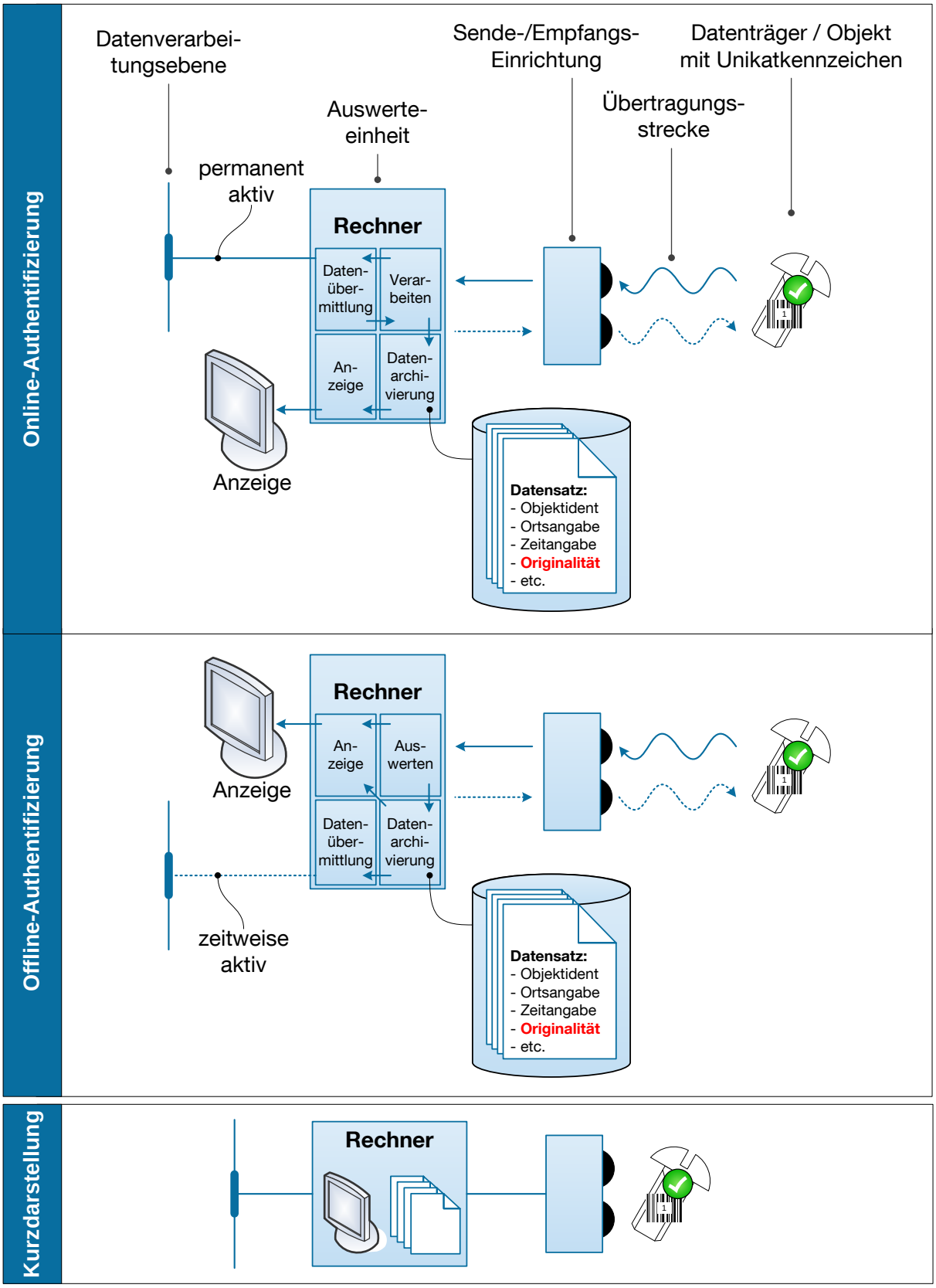


Abbildung 8-2: Aufbau eines IP-Punktes in Form einer Online- bzw. Offline-Authentifizierung

Prüfdatensatz eines IP-Punktes

Einstufung	Argument
Muss	Identität (weltweit eindeutige Objektidentifikationsnummer, z. B. UII / EPC)
Muss	Zeitangabe der Prüfung (Datum, Uhrzeit)
Muss	Ortsangabe der Prüfung
Muss	Originalitätsangabe als Ergebnis der Authentifizierung („Original“ oder „kein Original“)
Kann	Angabe des verwendeten Sicherheitsmerkmals [1]
Kann	Auflösung des UII / EPC in die Einzelargumente [2] • Identifikationsnummer des Nummerngebers (= Hersteller) • Objektnummer (= Sachnummer) • Seriennummer (vom Hersteller vergeben)
Kann	Identifikationsnummer des Erzeugers des Datensatzes
Kann	Identifikationsnummer des IP-Punktes (z. B. Seriennummer des Lesegerätes)
Kann	weitere Daten

[1] hilft bei der Auswertung und Bewertung der Qualität der Daten

[2] erleichtert die Auswertung der Datenbank bei Anfragen

Abbildung 8-3: Prüfdatensatz eines IP-Punktes

Bei einer Offline-Authentifizierung, wie diese im zweiten Teil der Abbildung 8-2 dargestellt ist, erfolgt die Authentifizierung auf Basis des gelesenen Sicherheitsmerkmals lokal in der Auswerteeinheit. Die Auswerteeinheit verarbeitet hierfür das erhaltene Signal mit dem zur Authentifizierung lokal gespeicherten Algorithmus. Auch bei der Offline-Authentifizierung ist es wichtig, dass das Ergebnis der Authentifizierung dem Nutzer an der Anzeige des IP-Punktes unmittelbar visualisiert wird. Beispiele für eine Offline-Authentifizierung sind in Abbildung 7-26, S. 169 und in Abbildung 7-27, S. 170 gegeben, können aber bei den in Anhang D abgebildeten Sicherheitsmerkmalen teilweise mittels technischer Prüfhilfsmittel sehr einfach erfolgen[29]. Für den Nachweis und für das Nachvollziehen der erfolgten Prüfungen wird auch in diesem

[29] siehe Anhang D, Spalte „Prüfaufwand (Hilfsmittel)“, Ausprägungen „portabel“ und „festinstalliert“, sofern in Spalte „Infrastruktur für Prüfung“ nicht „Datenverb.“ angegeben ist

Fall je Prüfvorgang ein Datensatz angelegt und lokal gespeichert. Sobald die Datenverbindung des IP-Punkts aktiviert ist, werden die gesammelten und noch nicht übermittelten Datensätze an die zentrale Datenarchivierung und -auswertung weitergegeben, sofern diese Datensätze dafür freigegeben sind.

Für die Erzeugung und lokale Speicherung des Prüfdatensatzes eignet sich die Auszeichnungssprache XML besonders gut. Je Prüfvorgang kann eine XML-Datei geschrieben und lokal gespeichert werden. Um die Prüfhistorie lokal nachzuvollziehen, können die abgespeicherten XML-Dateien eingesehen und gelesen werden. XML-Dateien sind sowohl durch Bediener, als auch Maschinen lesbar (siehe Abbildung 3-6, S. 49). Eine lokale, softwaregestützte Auswertung der gespeicherten XML-Dateien ist damit ebenso möglich. Dies ist für den Bediener etwas komfortabler. Die lokal abgelegten XML-Dateien können darüber hinaus direkt an die zentrale Datenarchivierung und -auswertung übertragen und dort in ein entsprechendes Datenbanksystem übertragen werden.

An einem IP-Punkt können mehrere Sende- / Empfangseinrichtungen zur Authentifizierung verschiedener Sicherheitsmerkmale angeschlossen sein. Dies ist in Abbildung 8-4 unter Benutzung der Kurzdarstellung aus Abbildung 8-2 schematisch dargestellt. Bezüglich der Kombination der Technologien gibt es hierbei keine Restriktionen und es können manuelle, halbautomatische sowie automatische Systeme verwendet werden (Definitionen siehe Anhang C.12). Es muss jedoch bei der Verwendung von Originalitätskennzeichen beachtet werden, dass auch die Identität der Ware festgestellt werden können muss, um einen korrekten Datensatz zur Realisierung der angestrebten T&T-Funktion erstellen zu können. Dafür eignet sich das in Abschnitt 7.3, S. 158 abgebildete Vorgehen zur Kombination von Identitäts- und Originalitätskennzeichen.

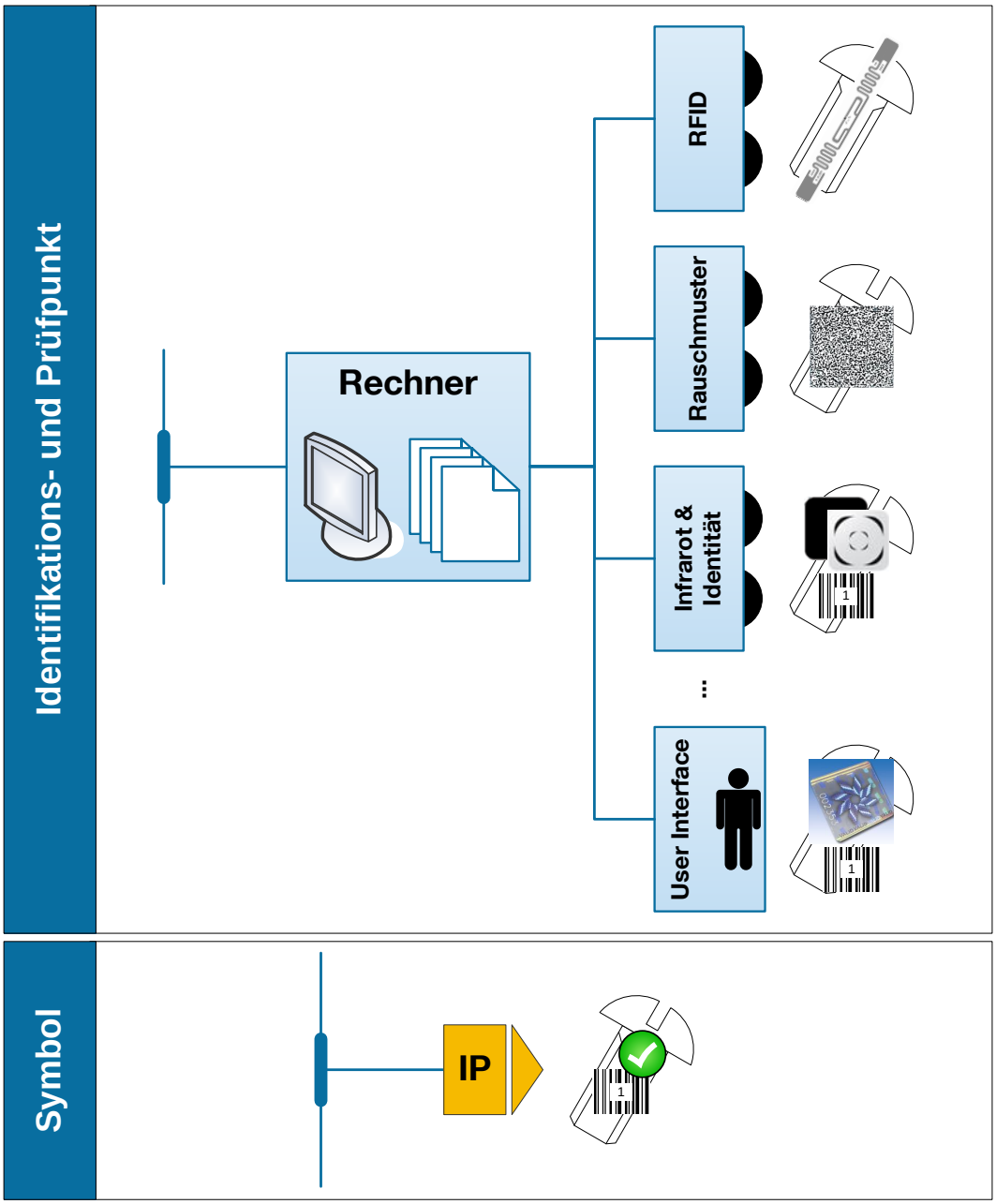


Abbildung 8-4: **Integration verschiedener Authentifizierungstechnologien an einem IP-Punkt mit vier verschiedenen Beispieltechnologien (Bildquellen Sicherheitsmerkmale: [Ali-13a, Gün-11a, Aus-13a, Sch-13a])**

Wie in Abschnitt 7.1.2.1, S. 110 dargestellt, erhöht eine (halb-)automatische Prüfung der Originalität eines Produkts die Sicherheit des Systems gegenüber einer manuellen Prüfung. Dies kann einerseits bei der Auswahl der je schützenswertem Bauteil passenden Sicherheitstechnologien nach der Methode in Abschnitt 7.1, S. 107 berücksichtigt werden. Allerdings ist es andererseits möglich, die Authentifzierungstechnologien entsprechend weiterzuentwickeln und Prüfgeräte für eine (halb-)automatische Prüfung zu qualifizieren. Ein Beispiel dafür ist in Abbildung 8-5 zu sehen. Die Anbindung eines passenden Lesegerätes an eine Auswerteeinheit mit Informa-

tionsübertragung konnte innerhalb der Forschung für diese Arbeit erstmals erfolgreich eingerichtet werden.

Handgerät

Visuelle Anzeige des Prüfergebnisses an einer Leuchtdiode

Halbautomatische Lösung

Halbautomatischer IP-Punkt mit visueller Anzeige des Prüfergebnisses sowie automatischer Übertragung an die Auswerteeinheit

Abbildung 8-5: Weiterentwicklung eines Handgeräts zu einer halbautomatischen Lösung zur Integration an einem IP-Punkt (Bildquelle Handgerät: [Sch-13a])

Bei rein manuell zu prüfenden Sicherheitsmerkmalen muss die Authentifizierung von qualifizierten Mitarbeitern vorgenommen werden. Das Ergebnis kann auch in diesem Fall datentechnisch erfasst werden, indem das Ergebnis der Authentifizierung an einer Eingabemaske eingegeben wird (siehe „User Interface“ in Abbildung 8-4). Bei Kombination mit einem maschinenlesbaren Identitätsmerkmal kann die Identität (also UII / EPC, siehe Abschnitt 7.4.1, S. 161) durch einen Scan ergänzt werden oder es erfolgt bei nicht-maschinenlesbaren Identitätsmerkmalen ebenfalls eine manuelle Eingabe durch den Mitarbeiter.

Zur Darstellung eines IP-Punktes auch mit mehreren Identifikations- und Authentifizierungstechnologien wird das in Abbildung 8-4 eingeführte Symbol in den nachfolgenden Systembeschreibungen verwendet.

8.3 IT-System zur Datenarchivierung und -auswertung

8.3.1 Verteiltes IT-System zur Datenerfassung

Wie in einem klassischen T&T-System werden im Produktpiraterie-Schutzsystem die IP-Punkte an transportrelevanten Schritten (z. B. Warenausgang, Wareneingang, Verladung, Entladung) platziert (siehe Abschnitt 3.2.1, S. 41). Um das Ziel des direkten Schutzes von Maschinen und Anlagen durch Authentifizierung eingebauter Ersatzteile und Komponenten zu erreichen (siehe Abschnitte 1.2.2, S. 8 und 5.4.2, S. 96), werden die IP-Punkte insbesondere auch in Maschinen und Anlagen eingebaut (siehe Abbildung 8-6). Diese IP-Punkte sind mit der Maschinen- / Anlagensteuerung gekoppelt und authentifizieren Bauteile beim Maschinenstart. Dies geschieht im besten Fall vollautomatisch. Es kann aber auch am Bedienterminal eine Aufforderung zur Prüfung an den Maschinenbediener ausgegeben werden, der dann eine halbautomatische oder manuelle Prüfung der angegebenen Bauteile vornimmt. Das ist vom gewählten Sicherheitsmerkmal und der damit verbundenen Prüftechnologie abhängig.

In den in Maschinen und Anlagen eingebauten IP-Punkten werden die Ergebnisse der einzelnen Authentifizierungen, wie in Abschnitt 8.2 beschrieben, als Datensatz gespeichert. Genau in diesem Fall ist das lokale Speichern der Daten von größter Wichtigkeit, da damit Gewährleistungsansprüche und Ansprüche aus Verfügbarkeitsgarantien zweifelsfrei geklärt werden können. Dies ist für beide Seiten äußerst wertvoll: einerseits für den Kunden, der zeigen kann, dass in dieser Maschine / Anlage lediglich Originalbauteile im Einsatz waren und sein Anspruch zu Recht besteht, andererseits für den Originalhersteller, der sich bzgl. der Verwendung von Komponenten und Ersatzteilen während der bisherigen Laufzeit sicher sein kann. Um dies im zeitlichen Verlauf klar zu dokumentieren, sollte die Maschine / Anlage neben den Prüfdatensätzen, die beim Maschinenstart geschrieben werden, auch Datensätze ablegen, die beim Abschalten der Maschine erzeugt werden.

Für die Rückverfolgbarkeit der einzelnen Komponenten und Ersatzteile bis zum Produktionszeitpunkt ist es sinnvoll, dass der Originalhersteller einen initialen Datensatz

anlegt, in dem der Herstellungszeitpunkt und der genaue -ort zusammen mit dem Ident des Bauteils abgelegt sind (siehe Abbildung 8-6). Weitere Daten können in diesem Datensatz zusätzlich ergänzt werden (siehe Abbildung 8-7). Insbesondere sollte lückenlos und nachweisbar gespeichert werden, dass das Sicherheitsmerkmal bei Abschluss des Herstellungsprozesses funktionsfähig integriert ist. Dies ist für die Belastbarkeit der Authentifizierung bei im Extremfall gerichtlichen Auseinandersetzungen notwendig (siehe „Eckpunkte für den optimalen Markierungsprozess“ in Abschnitt 7.5.1, S. 173).

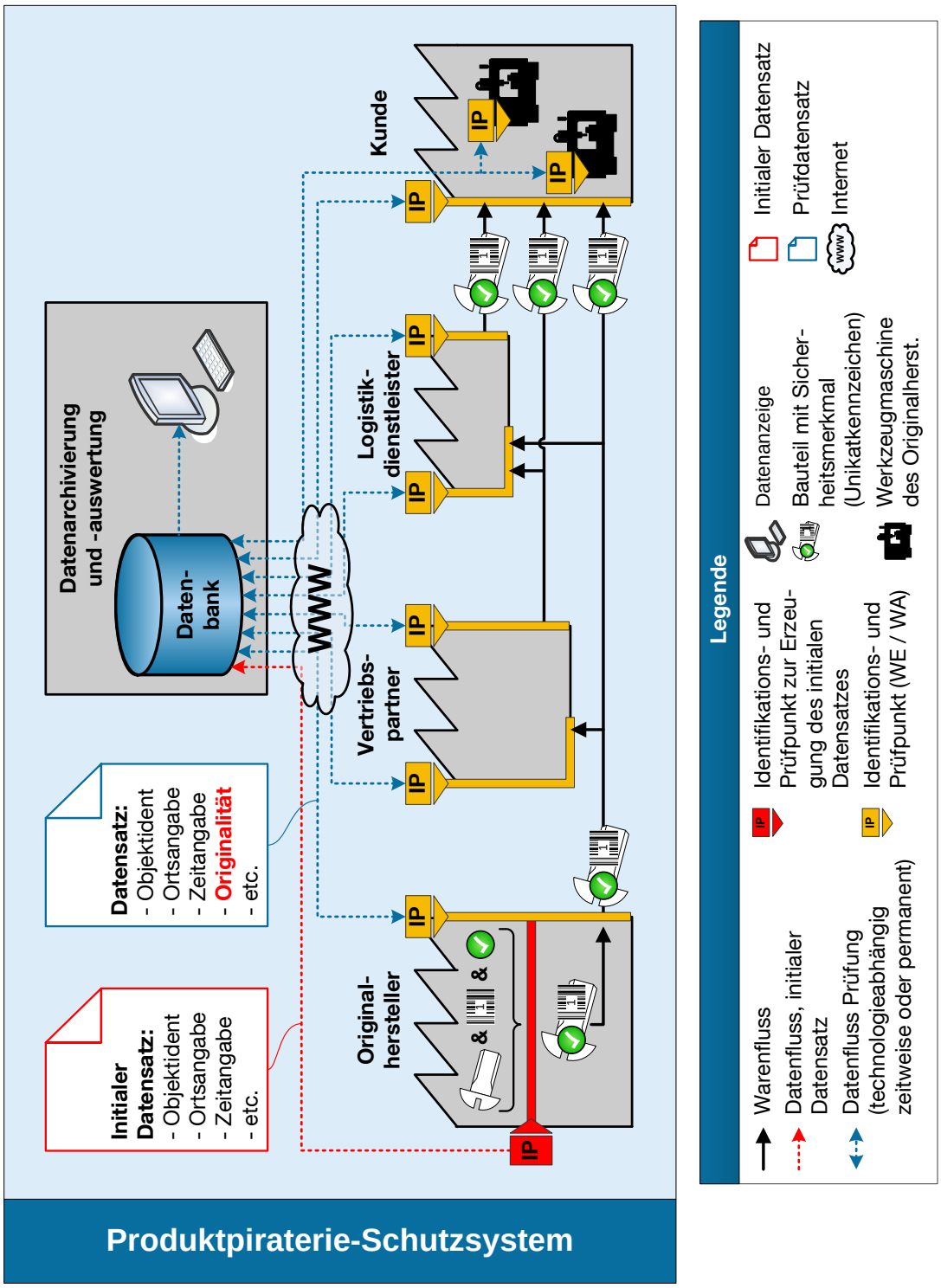


Abbildung 8-6: Schematischer Aufbau des Produktpiraterie-Schutzsystems, in Anlehnung an Abbildung 5-2, S. 86

Initialer Datensatz des Originalherstellers

Einstufung	Argument
Muss	Identität (weltweit eindeutige Objektidentifikationsnummer, z. B. UII / EPC)
Muss	Zeitangabe der Herstellung (Datum, Uhrzeit)
Muss	Ortsangabe der Herstellung
Muss	Originalitätsangabe als Ergebnis der Authentifizierung („Original“ oder „kein Original“)
Kann	Angabe des verwendeten Sicherheitsmerkmals [1]
Kann	Auflösung des UII / EPC in die Einzelargumente [2] • Identifikationsnummer des Nummerngebers (= Hersteller) • Objektnummer (= Sachnummer) • Seriennummer (vom Hersteller vergeben)
Kann	Identifikationsnummer des Erzeugers des Datensatzes
Kann	Identifikationsnummer des IP-Punktes (z. B. Serialnummer des Lesegerätes)
Kann	weitere Daten

[1] hilft bei der Auswertung und Bewertung der Qualität der Daten

[2] erleichtert die Auswertung der Datenbank bei Anfragen

Abbildung 8-7: Initialer Datensatz des Originalherstellers

8.3.2 Datenbanksystem

Es gibt vielfältige Möglichkeiten, wie die im vorgestellten verteilten Produktpiraterie-Schutzsystem gesammelten Daten in einem Datenbanksystem organisiert und gespeichert werden können. Dies ist Teil eines gesamten Wissenschaftsbereichs und kann in der einschlägigen Literatur nachgelesen werden [beispielsweise BSI-13d, Fac-13, Fae-07, Tan-08, Unt-12]. An dieser Stelle wird lediglich ein kurzer Überblick gegeben, welche Entitäten und Daten in einem vollständigen System zu berücksichtigen sind. Dies soll die Arbeitsgrundlage für ein Unternehmen zur Entwicklung eines passenden Systems darstellen.

In Abschnitt 5.4.2 und 5.4.3 (S. 96 und 99) sind bereits entsprechende Anforderungen formuliert. Ergänzt um die Anforderungen, die sich aus der Struktur des verteilten Systems zum Produktpirateriesschutz und den an den IP-Punkten erzeugten Da-

tensätzen ergeben, lassen sich die in Abbildung 8-8 gelisteten Punkte zusammenfassen.

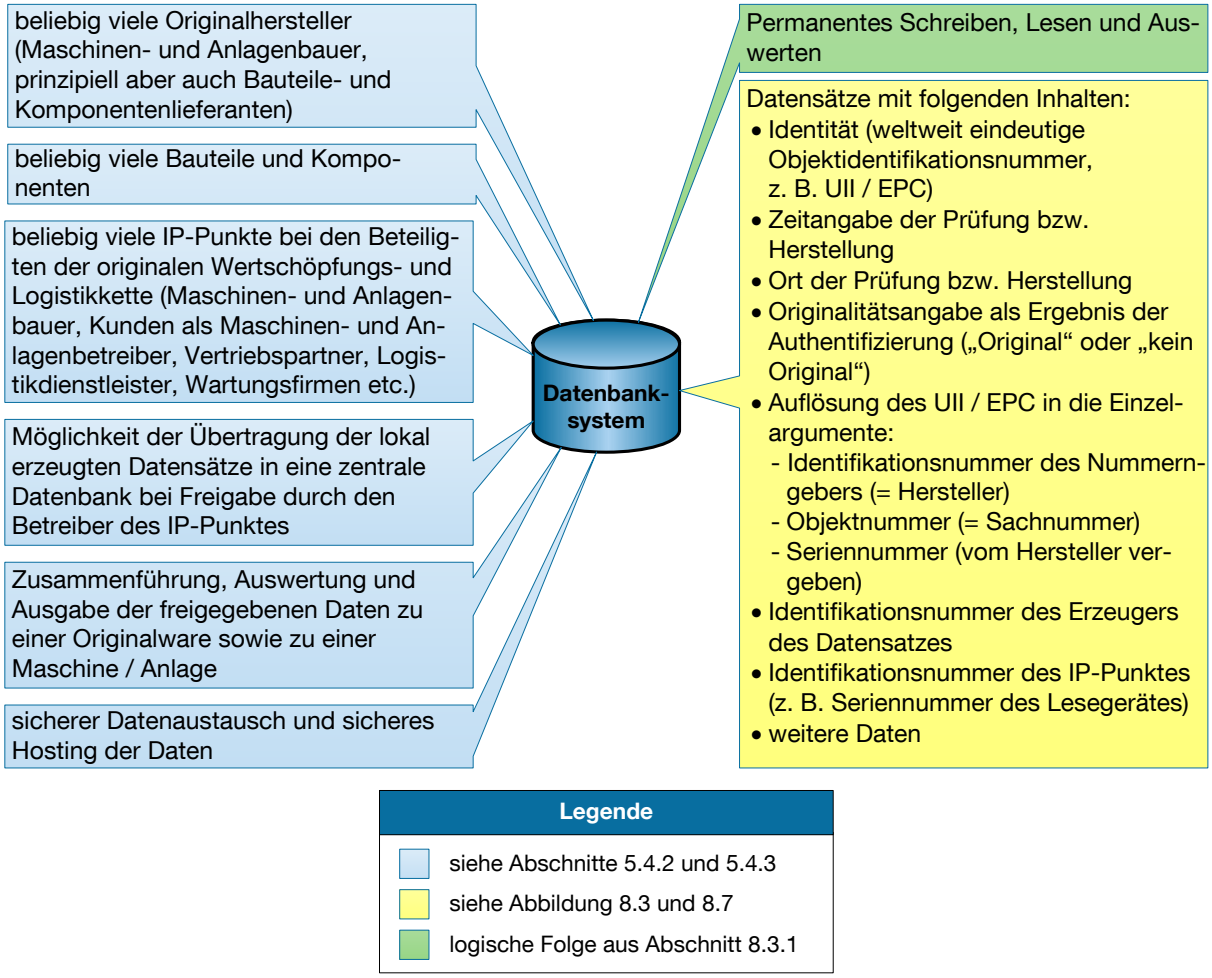


Abbildung 8-8: Anforderungen an die Funktionen und Struktur eines Datenbanksystems

Dabei ist eine zentrale Anforderung, dass sowohl die im verteilten System gespeicherten Daten (z. B. XML-Dateien lokal an den IP-Punkten, Daten im zentralen oder verteilten Datenbanksystem) als auch der Datenaustausch zwischen den Entitäten sicher gegen unbefugten Zugriff oder gar Manipulation sind. Dies kann beispielsweise mit den in Abschnitt 3.2.1.3, S. 50 dargestellten Maßnahmen erreicht werden.

Die Implementierung und Realisierung des Datenbanksystems ist als zentrale Lösung des Originalherstellers denkbar, der dann auch entsprechende Schnittstellen für die weiteren Beteiligten der Supply-Chain zur Verfügung stellen kann. Die Auswertung und die Auswerteergebnisse kann der Originalhersteller als Service für seine Kunden und Vertriebspartner anbieten und etablieren.

Eine andere Lösung wäre eine IT-as-a-Service-Lösung, bei der ein Drittanbieter das verteilte IT-System (Hardware sowie Software) einrichtet, betreibt und den Beteiligten der gesamten Wertschöpfungskette gegen Entgelt zur Verfügung stellt. In diesem Fall wäre es auch denkbar, dass beliebig viele Originalhersteller im System abgebildet werden und somit eine Branchen- und branchenübergreifende Lösung entsteht.

Unabhängig der konkreten Systemarchitektur oder des konkreten Betreibermodells muss dafür Sorge getragen werden, dass ein unternehmensübergreifend konsistentes Datenmodell für einen durchgängigen Datenaustausch verwendet oder etabliert wird. Ein Beispiel dafür wird in Abschnitt 8.4 gegeben.

8.3.3 Daten-Auswertesystem

Neben der Aussage an den eingerichteten IP-Punkten über die Originalität der unmittelbar und in der Vergangenheit geprüften Produkte ermöglicht das verteilte Produktpiraterie-Schutzsystem mit der integrierten Datenerfassung und -archivierung die Abfrage und Ausgabe wertvoller Daten für die jeweils berechtigten Nutzer. Wie die Zugriffsrechte modelliert, abgebildet und implementiert werden können, kann in einer rollenbasierten Zugriffskontrolle, wie in Abschnitt 3.2.1.3, S. 50 referenziert, geregelt sein. Zentrale Abfrage- und Ausgabedaten sind:

- Ausgabe der T&T-Daten zu einem einzelnen Bauteil inklusive sämtlicher Prüfergebnisse bzgl. dessen Originalität zur Beantwortung der Fragen:
    - Wann wurde das Bauteil hergestellt und ausgeliefert?
    - Welchen Weg nahm das Bauteil durch die Supply-Chain?
    - Wo befindet sich das Bauteil aktuell?
- Auswertung und Visualisierung der aktuellen Bestückung einer Maschine / Anlage bzgl. der markierten und in der Maschine / Anlage mittels der installierten IP-Punkte geprüften Komponenten und Ersatzteile zur Beantwortung der Frage:
    - Sind die aktuell eingebauten und überwachten Bauteile Originale?

  Diese Frage kann auch aus den lokal abgelegten Daten beantwortet werden.
- Auswertung und Visualisierung der Historie der Bestückung einer Maschine / Anlage bzgl. der markierten und in der Maschine / Anlage mittels der installierten IP-Punkte geprüften Komponenten und Ersatzteile als Antwort auf die Fragen:

  - Waren auf der betreffenden Maschine / Anlage in der Historie lediglich Originalbauteile im Einsatz?
  - Konnte in der Vergangenheit ein Bauteil nicht als Original bestätigt werden?
  - Gibt es zeitliche Lücken, in denen kein Bauteil gelesen wurde?

  Diese Fragen können auch aus den lokal abgelegten Daten beantwortet werden.
- Analysen und Plausibilitätschecks auf den Datenbeständen zur weiteren Erhöhung der Sicherheit im Gesamtsystem zur Beantwortung der Fragen:
  - An welcher Stelle tauchen Kopien auf?
  - Welche Produkte sind zur selben Zeit an unterschiedlichen Orten (Hinweis auf die Existenz von Kopien)?

Beispiele zur Verwendung und Visualisierung sind in Abbildung 8-12 und Abbildung 8-15 sowie in Abschnitt 9.1, S. 215 gegeben.

8.4 Implementierung des Produktpiraterie-Schutzsystems als Erweiterung des EPCglobal Network

Das in den Abschnitten 8.1 bis 8.3 beschriebene Produktpiraterie-Schutzsystem mit seinen Entitäten „logistische Einheiten“, „Identifikations- und Prüfpunkte“, „IT-System zur Datenarchivierung und -auswertung“ sowie der „Datenübertragung“ zwischen diesen Elementen könnte als neues, verteiltes System entwickelt, implementiert und errichtet werden. Für einen einzelnen Originalhersteller, der seine Maschinen und Anlagen entsprechend ausrüsten und passende Services für die Kunden, die weiteren Beteiligten der Supply-Chain sowie für seine eigene Weiterentwicklung einrichten möchte, ist dies sicherlich möglich.

Eine solche Insellösung hat ihre Vorteile beispielsweise in der Flexibilität, der leichten Abbildbarkeit bereits existierender unternehmens- und Supply-Chain-interner Prozesse sowie etablierter Standards und Nummernkreise. Dieser Lösung stehen jedoch auch die folgenden Nachteile gegenüber [Sto-11]:

- Nutzung von lediglich unternehmenseigenen Nummernkreisen möglich
- aufwendige Programmierung und Einrichtung unternehmensindividueller Software sowie deren Wartung und Weiterentwicklung
- Konzeptionierung und Einrichtung unternehmensspezifischer Datenbanken

- T&T von Objekten auf eigene Supply-Chain begrenzt
- örtliche Begrenzung der Steuerung von Prozessen

Bei einer IT-as-a-Service-Lösung, bei der in einer Supply-Chain-übergreifenden Lösung mehrere Originalhersteller mit ihrem Wertschöpfungsnetzwerk abgebildet und integriert werden können (siehe Abschnitt 8.3.2), besteht die Notwendigkeit der Standardisierung von Nummernkreisen und Datenbezeichnern [Sto-11]. Dies betrifft also insbesondere die Entwicklung eines einheitlichen Datenmodells mit einer durchgängigen Definition der einzelnen Bezeichner, Austauschformate und -protokolle, was einen sehr großen Aufwand darstellt. Allerdings kann in diesem Fall ein existierender Standard verwendet werden.

Der internationale Standardisierungsdienstleister GS1 [siehe GS1-13a] hat ein Netzwerk entwickelt, das es den Wirtschaftsbeteiligten ermöglicht, den Aufenthaltsort von Waren in der Supply-Chain nahezu in Echtzeit dokumentieren und feststellen zu können. Dieses Netzwerk heißt „EPCglobal Network“. Dabei ist explizit auch der leichte Austausch weiterer Informationen über diese Waren, wie beispielsweise das Herstell- oder Verfallsdatum, vorgesehen. [Fin-12 S. 368 f.]

Die Vorteile des EPCglobal Networks sind [Sto-11]:

- Weltweit eindeutige Identifizierbarkeit von Produkten, logistischen Einheiten, Transporthilfsmitteln, Dokumenten und Akten, Orten, Investitionsgütern sowie Dienstleistungen
- Durchgängige Identifikation von Produkten entlang der gesamten Supply-Chain (ohne Umetikettierung)
- Transparenz von Beständen, Materialflüssen, Geschäftsprozessen im gesamten Wertschöpfungsnetzwerk mittels standardisierter verteilter Datenbanken
- Steuerung der Prozesse auf Basis von Daten der vollständigen Supply-Chain

Als Erweiterung des EPCglobal Network können im vorliegenden Fall die Angaben zur Originalität eines Produktes als zusätzliche Informationen innerhalb des Netzwerks ausgetauscht werden.

8.4.1 Das EPCglobal Network

Um innerhalb des EPCglobal Network den Aufenthaltsort von Waren in der Supply-Chain nahezu in Echtzeit dokumentieren und feststellen zu können, bedient sich die-

se Technologie des Internets und stellt weitere Dienste zur Verfügung [GS1-13d, Fin-12 S. 368 f., Ver-05 S. 4]. Das EPCglobal Network wurde vom Auto-ID Center[30] des Massachusetts Institute of Technology (MIT) entwickelt [Sar-00] und besteht aus drei wesentlichen Komponenten [siehe GS1-13d S. 29, 31, 36 ff., Ver-05, Ver-08]:

- Object Naming Service (ONS):
  Der ONS ist ein Verzeichnis von Unternehmen mit ihren Manager IDs sowie ihren registrierten lokalen ONS, welche Verweise auf die herstellereigenen EPCIS speichern. Die Manager IDs sind mehrheitlich identisch mit den Company Prefixes (siehe Abschnitt 3.2.1.1, S. 44), es gibt aber im Standard vorgesehene Ausnahmen.
- EPC Information Services (EPCIS):
  Die EPCIS sind Datenbanken, in denen die Teilnehmer einer Supply-Chain Informationen wie statische (Produkt-)Daten sowie logistische (Bewegungs-) Daten über einmalige logistische Einheiten in der Supply-Chain speichern und teilen.
- EPC Discovery Service:
  Der EPC Discovery Service ist ein Registrierungsservice mit einem Verzeichnis über alle EPCIS der Teilnehmer einer Supply-Chain, die zu einer einmaligen logistischen Einheit Informationen beinhalten.

Sobald ein Hersteller ein Erzeugnis produziert und mit einem EPC kennzeichnet (siehe Abschnitt 7.4.1, S. 161), legt er in seinem unternehmenseigenen EPCIS-Repository Daten zu diesem Produkt ab, beispielsweise den EPC zusammen mit der Zeitangabe der Herstellung und Chargennummer (siehe Abbildung 8-9). Gleichzeitig registriert der EPC Discovery Service, dass im EPCIS-Repository des Herstellers Daten zu diesem speziellen EPC existieren [Fin-12 S. 376, Ver-05 S. 6].[31]

Sobald ein weiterer Teilnehmer der Supply-Chain dieses Produkt in seinem Unternehmen identifiziert, wird ebenfalls ein neuer Datensatz im unternehmenseigenen EPCIS-Repository für dieses Produkt angelegt. Auch in diesem Fall erfolgt gleichzeitig eine Registrierung im EPC Discovery Service, dass im eigenen EPCIS-Repository

[30] Dieses Auto-ID-Center wurde später aufgeteilt in die EPCglobal Inc., heute GS1 [Fin-12 S. 368], und die Auto-ID Labs [Mey-08].

[31] Um eine durchgängige Benennung der Daten zu erhalten, wurden entsprechende Bezeichner im „Core Business Vocabulary Standard" formuliert [EPC-10].

(Bewegungs-)Daten zu diesem speziellen EPC existieren. Die weiteren Beteiligten der Supply-Chain agieren identisch. [Fin-12 S. 376 f., Glo-06 S. 176 ff., Ver-05 S. 6]

Zusätzlich wird vor Vergabe des ersten EPC der Hersteller von Produkten im ONS mit seinem lokalen ONS registriert. So können autorisierte Herstellerangaben zu einem vorliegenden Produkt jederzeit direkt vom EPCIS des Herstellers abgerufen werden. [Glo-06 S. 178 ff., GS1-13d S. 8, S. 37 ff., Kuh-07 S. 6 ff., Ver-05 S. 6]

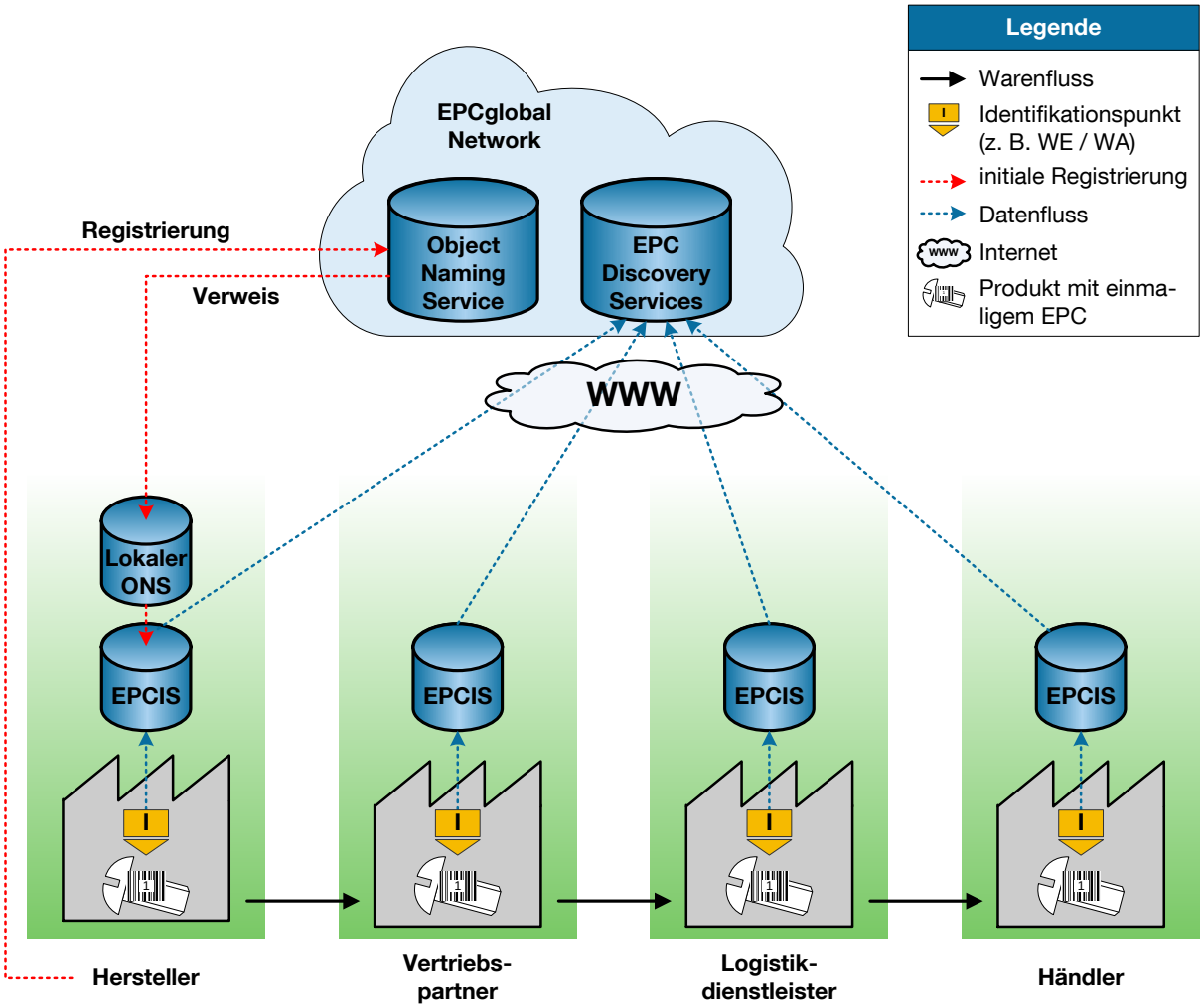


Abbildung 8-9: EPCglobal Network, in Anlehnung an [Fin-12, Sto-11, Ver-05]

Der Standard für den EPC Discovery Service ist aktuell noch in Entwicklung [siehe GS1-13d S. 11, S. 36, S. 57, GS1-13e], weshalb die Funktionen dieses Service noch nicht abschließend definiert sind. Zwei wesentliche Funktionen werden jedoch sein [GS1-13d S. 57f.]:

- Suchfunktion:
  Der EPC Discovery Service wird eine Suchfunktion anbieten, die es ermöglicht, die vielfältigen Quellen für Informationen bezüglich eines einmaligen Identitätsmerkmals (z. B. EPC) im EPCglobal Network zu finden – insbesondere dann, wenn die Informationen von verschiedenen Teilnehmern einer Supply-Chain zur Verfügung gestellt werden.
- Authentifizierungsfunktion:
  Der EPC Discovery Service wird eine Funktion abbilden, die es ermöglicht, einen zugreifenden Nutzer zu authentifizieren und gleichzeitig dessen Rechte bezüglich des Zugriffs auf die angeforderten Daten zu überprüfen.

Sollte ein Teilnehmer der Supply-Chain – beispielsweise der Händler – genauere Informationen über ein vorliegendes Produkt abrufen wollen, gibt es für ihn zwei Möglichkeiten [GS1-13d S. 36 ff.]:

- Abruf von Herstellerangaben:
  Die Anfrage des Nutzers geht an den ONS. Der ONS teilt die Adresse des lokalen ONS mit, der wiederum die Adresse des lokalen EPCIS des Herstellers kennt, in dem die Herstellerangaben gespeichert sind (Abbildung 8-10).
- Abruf von Bewegungsdaten:
  Die Anfrage des Nutzers geht an den EPC Discovery Service. Der EPC Discovery Service hat zuvor bei der Bewegung des Produkts durch die Supply-Chain die Einträge der weiteren Beteiligten in die eigenen lokalen EPCIS-Repositories registriert und teilt die Adressen dieser Repositories nun an den Nutzer mit. Dieser ruft aus den lokalen EPCIS-Repositories die gewünschten Informationen ab, sofern die Berechtigung dafür besteht (Abbildung 8-11).

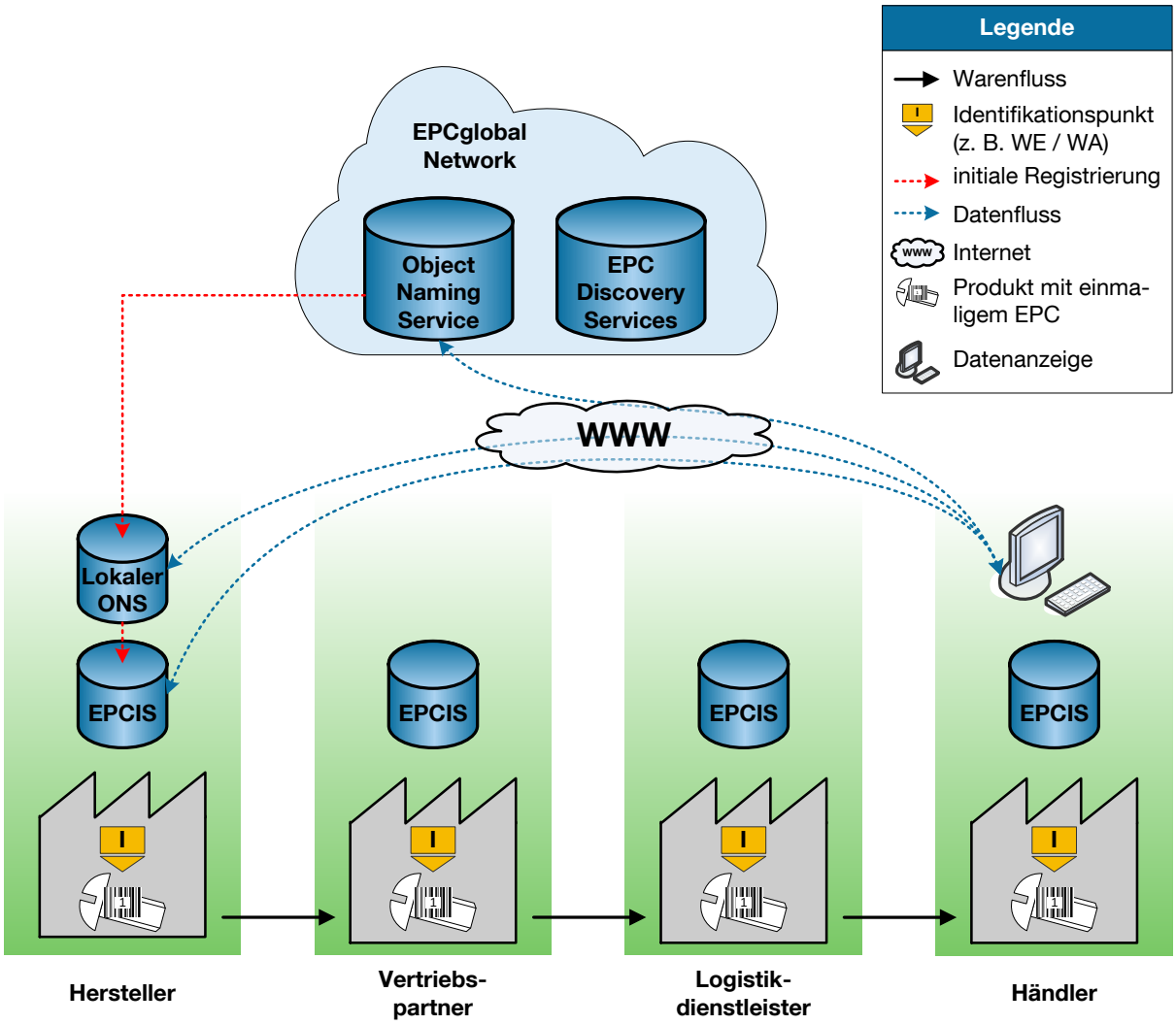


Abbildung 8-10: EPCglobal Network, Abruf von autorisierten Herstellerangaben, in Anlehnung an [Fin-12, Sto-11, Ver-05]

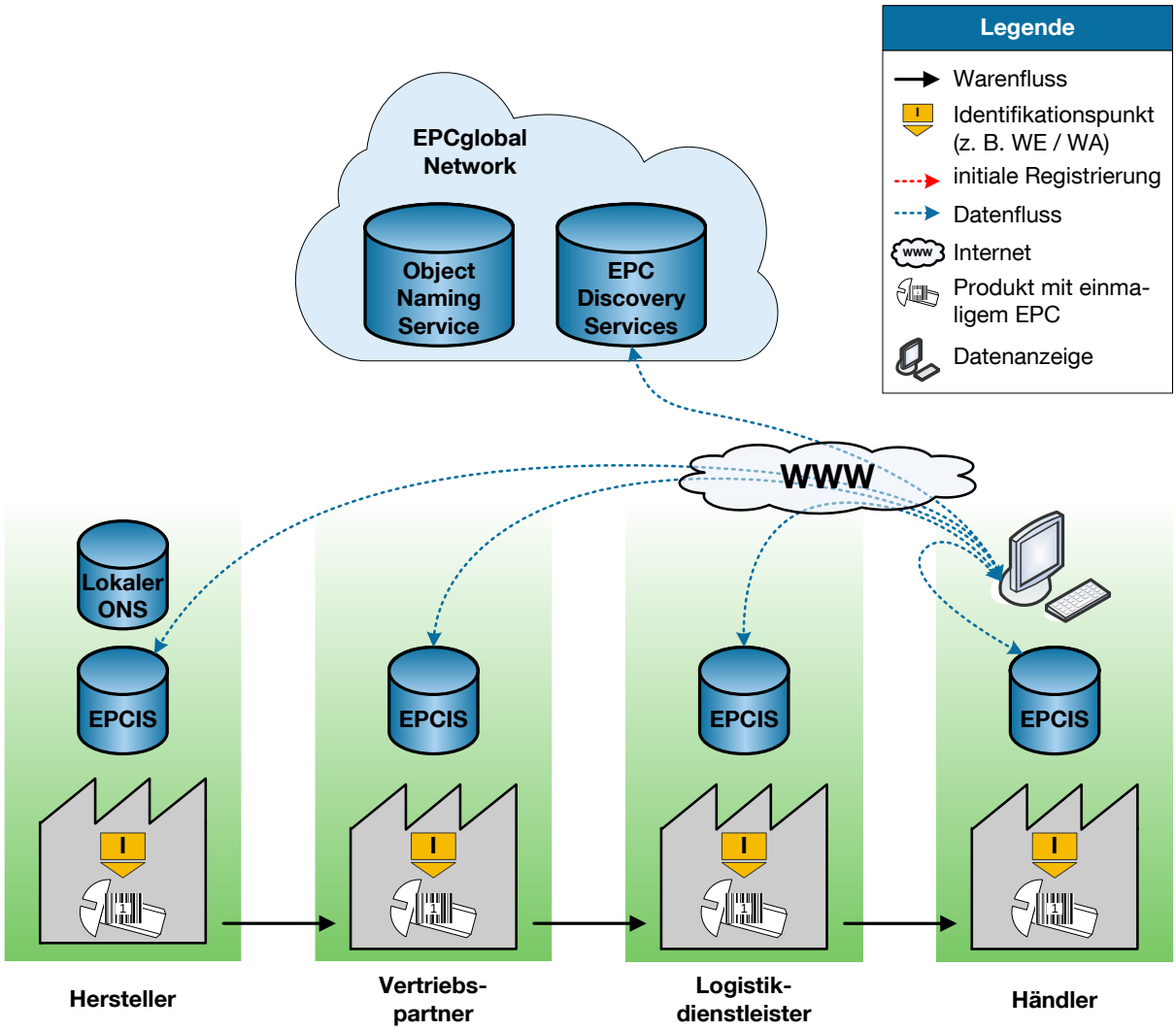


Abbildung 8-11: EPCglobal Network, Abruf von Bewegungsdaten, in Anlehnung an [Sto-11]

Seitens GS1 ist aktuell die Verisign Inc. mit Sitz in Reston, USA mit dem Betrieb des ONS sowie des EPC Discovery Service beauftragt [Ver-05 S. 8]. Geplant ist jedoch, dass es im EPCglobal Network verschiedene EPC Discovery Service Provider geben soll. Somit kann jeder Teilnehmer des EPCglobal Network seinen Provider frei wählen, der für ihn u. a. auch das Rechtemanagement verwaltet [GS1-13d S. 57].

8.4.2 Erweiterung zum Produktpiraterie-Schutzsystem

Das EPCglobal Network kann im Sinne des in dieser Arbeit entwickelten Produktpiraterie-Schutzsystems genutzt werden. Dabei kann RFID als Sicherheitsmerkmal zum Einsatz kommen (siehe Abschnitt 8.4.2.1), insbesondere jedoch auch prinzipiell jedes weitere Unikatkennzeichen (siehe Abschnitt 8.4.2.2). Das Unikatkennzeichen kann dabei technologiebedingt per se einmalig sein, oder sich, wie in Abschnitt 7.3,

S. 158 dargestellt, aus einem Originalitäts- und einem Identitätskennzeichen zusammensetzen.

8.4.2.1 RFID als Sicherheitsmerkmal

Bei Verwendung von RFID als Unikatkennzeichen ist es möglich, ein Produkt mit Hilfe eines EPC (siehe Abschnitt 7.4.1, S. 161) zu individualisieren und wiedererkennbar zu machen. Zudem ist es gleichzeitig möglich, den Transponder mit Sicherheitsfunktionen auszustatten (siehe Abschnitte 7.4, 160). Die Verwendung des EPC für die Funktion des T&T innerhalb des EPCglobal Network ist bereits beschrieben (siehe Abschnitt 8.4.1). Offen ist noch die Frage, wie das EPCglobal Network um die Funktion der Authentifizierung ergänzt werden kann.

Die Authentifizierung ist ein zusätzlicher Service, den der Originalhersteller anbietet. Dabei ist es prinzipiell egal, ob die Authentifizierung mit oder ohne Datenverbindung – also online oder offline – stattfindet. Denn die IP-Punkte haben einerseits die Funktion der Identifikation, die bei Teilnahme im EPCglobal Network nach den Standards von GS1, und andererseits die Funktion der Authentifizierung, die nach Vorgabe des Herstellers respektive der verwendeten Authentifizierungsform erfolgt.

Die IP-Punkte sind somit nach Abschnitt 8.2 in der Lage, die Identifikation eines Produkts durchzuführen, die Authentifizierung vorzunehmen und einen entsprechenden Datensatz mit den gewünschten Daten anzulegen (siehe Abbildung 8-2 und Abbildung 8-3). Dieser Datensatz wird nun in das lokale EPCIS-Repository des jeweiligen Teilnehmers übertragen. Somit liegen die Daten lokal für den jeweiligen Teilnehmer nachvollziehbar vor und diese Daten sind auch für jeden weiteren berechtigten Teilnehmer im EPCglobal Network sichtbar um weitere Funktionen erschließen zu können, z. B. T&T mit ergänztem Authentifizierungsergebnis je Bauteil oder je Maschine. Wie eine passende Visualisierung dazu aussehen kann, ist in Abbildung 8-12 dargestellt.

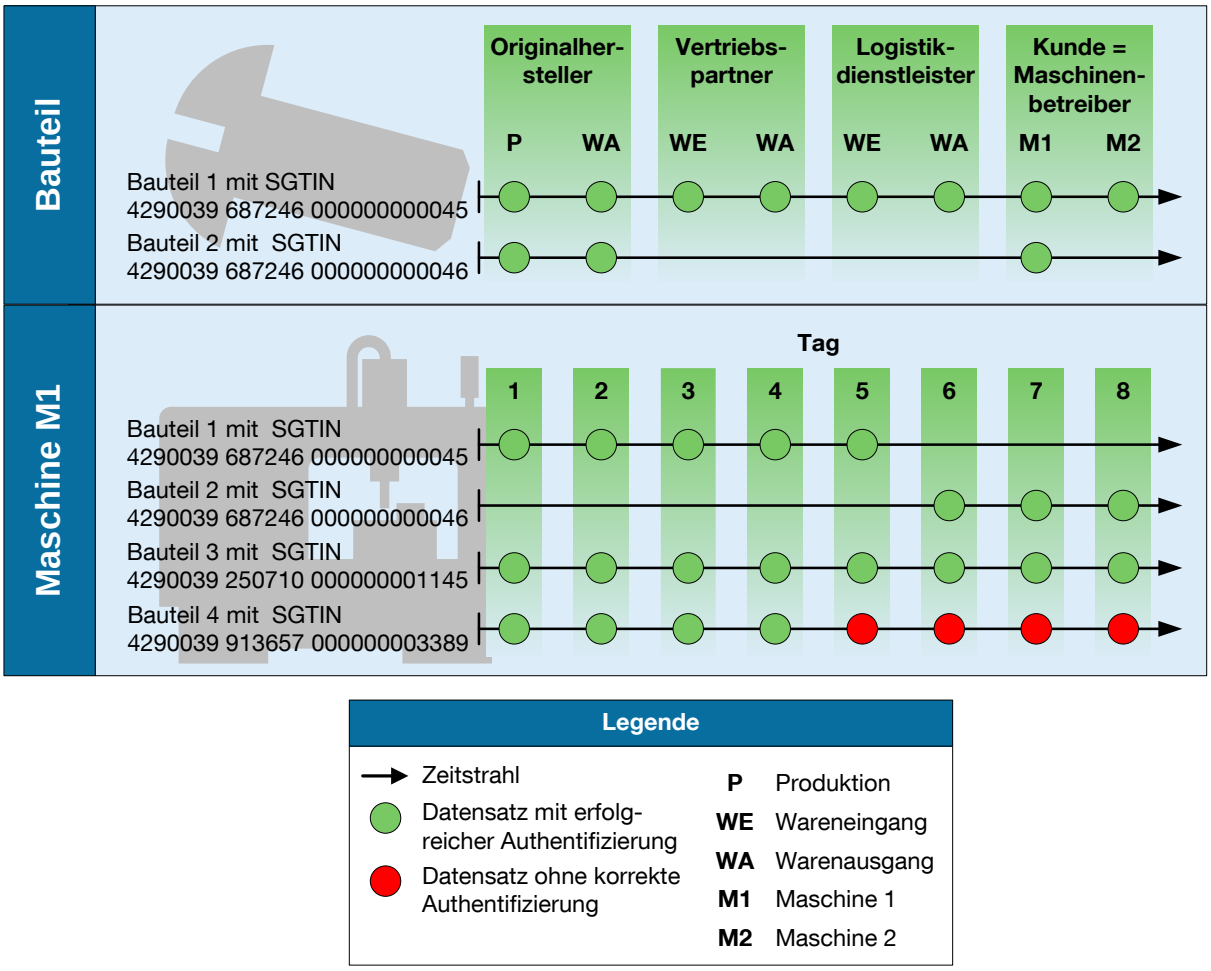


Abbildung 8-12: Visualisierung der T&T- in Kombination mit Authentifizierungsinformationen für kritische Bauteile mit Unikatkennzeichen, in Anlehnung an [Abe-10 S. 117] [32]

Als Datenaustauschformat zwischen den im EPCglobal Network beteiligten Entitäten wird seitens GS1 die Auszeichnungssprache XML verwendet. Der Aufbau der XML-Datensätze ist im Standard „EPC Information Services (EPCIS)“ [EPC-07] beschrieben und nutzt die Vorgabe für die XML Schema Sprache durch das World Wide Web Consortium (kurz W3C). In Abbildung 8-13 ist eine standardkonforme XML-Datei dargestellt. Neben den gemäß Standard definierten Attributen „eventTime” und „eventTimeZoneOffset”, „epcList” mit „epc“, „action” sowie „bizLocation“ [siehe EPC-07 S. 40, 42] sind noch weitere Daten angegeben, welche für Funktionalitäten des Produktpiraterie-Schutzsystems als standardkonform eingeführte Extensions [EPC-07] S. 21] hinzugefügt wurden:

[32] Die Anordnung der Authentifizierungsergebnisse ist lediglich beispielhaft und bezieht sich nicht auf reale Fälle.

- „tid“
  enthält die TID des Transponders (siehe Abschnitt 7.4.1, S. 161)
- „originality”
  enthält das Ergebnis der Authentifizierung mit den Werten „true“ oder „false“
- „readerid”
  enthält die Nummer des RFID-Lesegerätes
- „companyprefix”, „itemreference“ und „serialnumber“
  enthalten den EPC, zerlegt in seine Bestandteile (siehe Abschnitt 7.4.1, S. 161 mit Abbildung 7-23, S. 164)
- „machineid“
  enthält die Maschinennummer, sofern die Authentifizierung an einem IP-Punkt in einer Maschine, also im eingebauten Zustand stattgefunden hat
- „trustservice“
  enthält den Eintrag eines Prüfers, der bei manuell zu prüfenden Sicherheitstechnologien seine persönliche Nummer o. ä. angibt, um die Belastbarkeit des unter „originality“ eingetragenen Prüfergebnisses zu dokumentieren
- „technology“
  enthält die Angabe zum verwendeten Sicherheitsmerkmal

Das stufenweise Entstehen der Daten für eine XML-Datei für den Datenaustausch zwischen IP-Punkt und EPCIS-Repository ist in Abbildung 8-14 dargestellt. In diesem Beispielfall wird davon ausgegangen, dass RFID als Sicherheitsmerkmal verwendet wird und eine Offline-Authentifizierung mittels Signatur gemäß Abschnitt 7.4.4, S. 169 stattfindet. Der Rechner erzeugt am IP-Punkt die XML-Datei, welche dann unverändert in das EPCIS-Repository übertragen wird.

Beispiele schützenswerter Bauteile mit RFID als Unikatkennzeichen unter Verwendung einer Signatur sind in Abbildung 7-28, S. 176 zu sehen. Bei der Firma Multivac Sepp Haggenmüller GmbH & Co. KG wurden sowohl die Klammerkette als auch die Siegeldichtung mit RFID, bei der Firma Vollmer Werke Maschinenfabrik GmbH die Einmesslehre gekennzeichnet. Alle Transponder tragen die drei in Abbildung 8-14 dargestellten Argumente „epc“, „tid“ und „signatur“.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<epcis:EPCISDocument xmlns:epcis="urn:epcglobal:epcis:xsd:1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" schemaVersion="1.0"
xmlns:proauthent="http://de.tum.mw.fml.proauthent"
xmlns:epcglobal="urn:epcglobal:xsd:1" creationDate="2008-03-16T22:13:16.397+01:00"
xsi:schemaLocation="urn:epcglobal:epcis:xsd:1 EPCglobal-epcis-1_0.xsd">
    <EPCISBody>
        <EventList>
            <ObjectEvent>
                <eventTime>2013-05-02T11:48:26.187+01:00</eventTime>
                <eventTimeZoneOffset>+01:00</eventTimeZoneOffset>
                <epcList>
                    <epc>urn:epc:id:sgtin:4290039.687246000000000045</epc>
                </epcList>
                <action>OBSERVE</action>
                <bizLocation>
                    <id>Händler</id>
                </bizLocation>
                <proauthent:tid>01331000097D3827</proauthent:tid>
                <proauthent:originality>true</proauthent:originality>
                <proauthent:readerid>D8ED2712</proauthent:readerid>
                <proauthent:companyprefix>P4290039</proauthent:companyprefix>
                <proauthent:itemreference>P687246</proauthent:itemreference>
                <proauthent:serialnumber>P000000000045</proauthent:serialnumber>
                <proauthent:machineid/>
                <proauthent:trustservice/>
                <proauthent:technology>rfid</proauthent:technology>
            </ObjectEvent>
        </EventList>
    </EPCISBody>
</epcis:EPCISDocument>
```

Abbildung 8-13: Beispiel einer XML-Datei, erzeugt von einem IP-Punkt

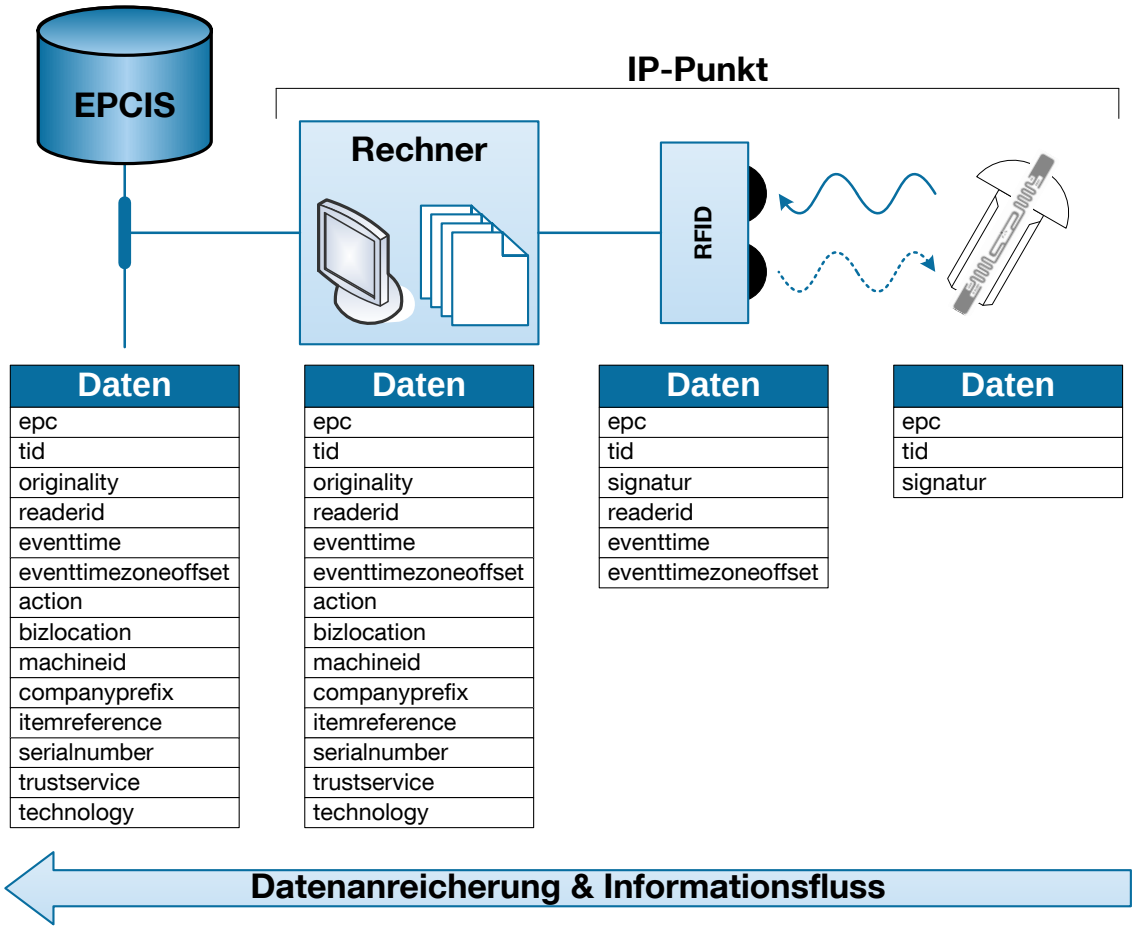


Abbildung 8-14: Beispiel für die Entstehung der Daten in einer XML-Datei an einem IP-Punkt unter Einsatz von RFID, in Anlehnung an [Gün-11c S. 24]

8.4.2.2 Verwendung weiterer Sicherheitstechnologien

Neben RFID können auch andere Sicherheitstechnologien verwendet werden, um am IP-Punkt Produkte zu identifizieren und zu authentifizieren. Dies sieht das EPCglobal Network explizit vor [GS1-13d S. 25, 46]. Wichtig ist, dass bei Verwendung eines anderen Sicherheitsmerkmals neben dem „epc“ sowie den weiteren standardmäßig geforderten Argumenten in der XML-Datei wenigstens auch „originality” mit einem Wert belegt werden kann. Dies ist mit dem Aufbau der IP-Punkte nach den Vorgaben in Abschnitt 8.2 möglich. Der Datenentstehungsprozess verläuft bei Verwendung einer anderen Technologie am IP-Punkt analog zu Abbildung 8-14.

Ein Beispiel eines schützenswerten Bauteils mit einem Unikatkennzeichen ist in Abbildung 7-28, S. 176 bei der Firma HOMAG Holzbearbeitungssysteme GmbH abgebildet. Die HSK-Schnittstelle der Bearbeitungsaggregate wurde hierzu mit einem Ringetikett mit Rauschmustercodes versehen. Diese beinhalten das Argument

„epc“. Die Authentifizierung erfolgt durch die Technologie des Rauschmustercodes (siehe Anhang A.5.5.5) lokal.

8.5 Nutzung des Produktpiraterie-Schutzsystems mit reinen Originalitätskennzeichen

Im Maschinen- und Anlagenbau ist es nicht immer sinnvoll, die als schützenswert eingestuften Ersatzteile oder Komponenten zu individualisieren. Dies liegt meist am Verhältnis zwischen dem Wert des Bauteils und den Kosten, die bei einer über die reine Sachnummernkennzeichnung hinaus gehenden Serialisierung entstehen. Es lohnt sich teilweise nicht, die Bauteile mit fortlaufenden Nummern zu kennzeichnen. Der Originalhersteller verwendet dann ein Originalitätskennzeichen (siehe Abschnitt 2.7.1, S. 27) meist in Verbindung mit der Sachnummer ohne Seriennummer.

Sofern das Produktpiraterie-Schutzsystem in der bisher beschriebenen Form aufgebaut ist, ist es dennoch sinnvoll, für die gekennzeichneten Bauteile innerhalb der Supply-Chain und insbesondere in den Maschinen bei der Authentifizierung entsprechende Datensätze anzulegen. So kann festgestellt werden, zu welchem Zeitpunkt an welchem IP-Punkt Bauteile nicht als Originale authentifiziert werden konnten. Dies sind für den Originalhersteller wie auch die weiteren Beteiligten der Supply-Chain wertvolle Informationen. Damit können ebenso gezielt Störungen in der Original-Supply-Chain erkannt und beseitigt werden, wie auch Nachweise für die Verwendung oder Nicht-Verwendung von Originalbauteilen in Maschinen / Anlagen erbracht werden. Ein Vorschlag für eine Visualisierung der Daten im gesamten Produktpiraterie-Schutzsystem zu Bauteilen mit Originalitätskennzeichen wird in Abbildung 8-15 gemacht. Ein Beispiel eines Bauteils mit einer reinen Originalitätskennzeichnung ist in Abbildung 7-28, S. 176 mit der Drahttransportrolle der Firma Vollmer Werke Maschinenfabrik GmbH gegeben.

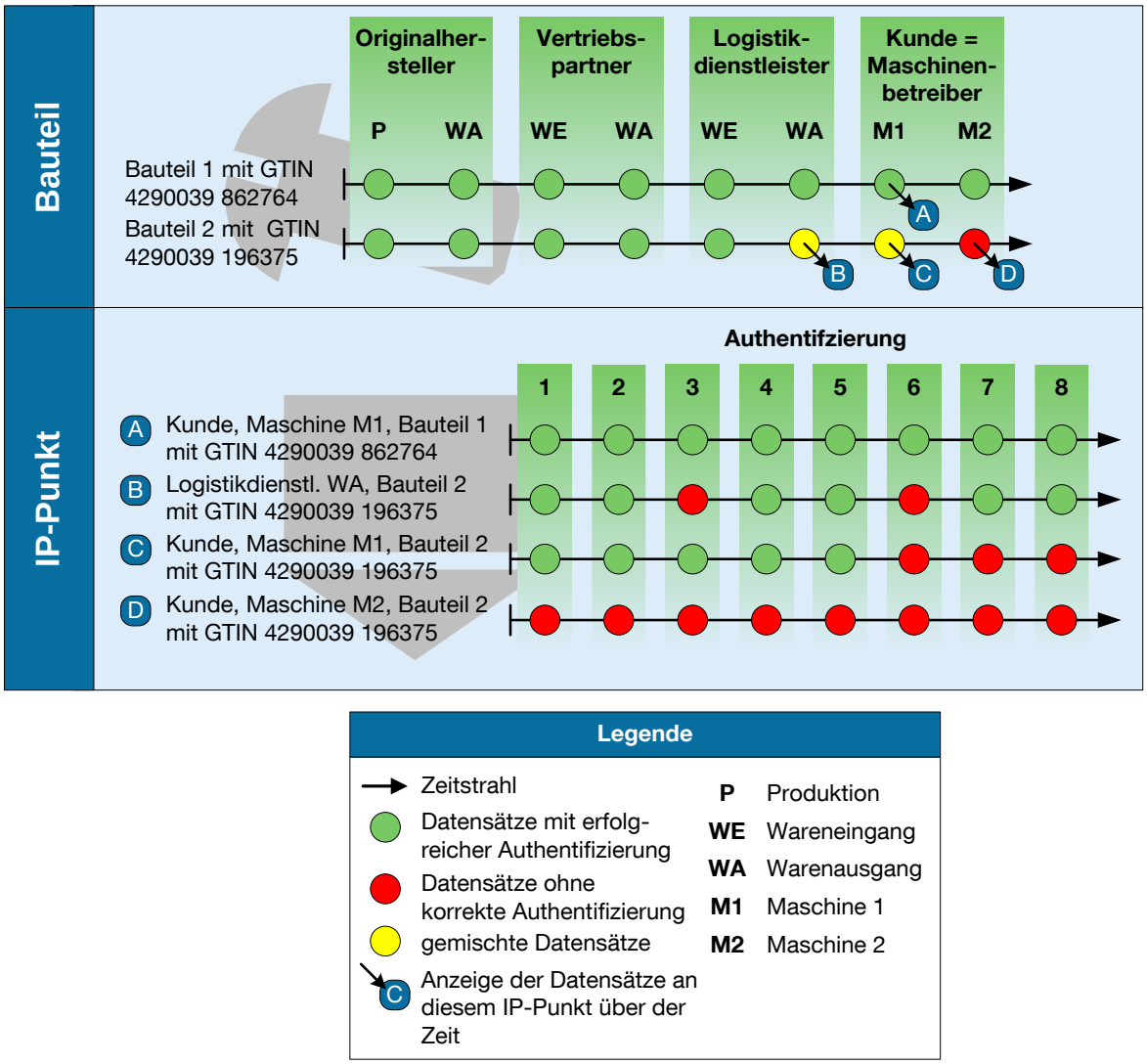


Abbildung 8-15: Visualisierung der Authentifizierungsinformationen für kritische Bauteile mit Originalitätskennzeichen [33]

8.6 Realisierung des verteilten Produktpiraterie-Schutzsystems in konkreten Umsetzungen

Das beschriebene verteilte Produktpiraterie-Schutzsystem konnte bereits pilothaft umgesetzt und die beschriebenen Funktionalitäten somit validiert werden. Für die Pilotinstallationen wurden dabei bewusst existierende Maschinen und Anlagen ausgewählt und die IP-Punkte dort installiert. Dies hat den Grund, dass die Integration eines IP-Punktes in eine Maschine / Anlage zur Authentifizierung eines eingebauten Bauteils größeren Anforderungen genügen muss (z. B. bezüglich Bauraum, Zugäng-

[33] Die Anordnung der Authentifizierungsergebnisse ist lediglich beispielhaft und bezieht sich nicht auf reale Fälle.

lichkeit, Umgebungsbedingungen) als dies bei einem IP-Punkt in der vorgelagerten Supply-Chain der Fall ist. Zudem ist der kritischste Punkt in der gesamten Supply-Chain der Verbau von Bauteilen in Maschinen / Anlagen, bei denen die Beteiligten bestätigt sehen wollen, dass es sich um Originale handelt.

Die in den Abschnitten 5.2.2, 7.1.3, 7.2.3 und 7.5.2 abgebildeten Beispiele (S. 89, 121, 157, 175) werden hier fortgesetzt. Für den erstmaligen Aufbau der IP-Punkte in Maschinen haben die Unternehmen HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG sowie Vollmer Werke Maschinenfabrik GmbH die Integration in ihre Maschinen vorgenommen. Dabei wurde der Aufbau aus Abbildung 8-2 realisiert. Das jeweilige schützenswerte Bauteil wurde mit dem jeweils ausgewählten Sicherheitsmerkmal versehen (siehe Abbildung 7-28, S. 176) und in die Maschine eingebaut. Ebenso wurde der IP-Punkt in die Maschine integriert: Platzierung der Sende- / Empfangseinrichtung an einer passenden Stelle und datentechnische Verbindung mit der Steuerung zur Erzeugung der Datensätze und deren Übertragung in eine Datenbank.

Die Realisierungen sind schematisch in Abbildung 8-16 dargestellt. Bei den Pilotinstallationen gibt es die Möglichkeit, die Daten von den Maschinen manuell durch einen Service-Mitarbeiter in das EPCIS-Repository oder automatisch über eine bestehende innerbetriebliche LAN-Verbindung übertragen zu lassen.

Als Darstellung einer realen Pilotinstallation wurde die Einmesslehre der Firma Vollmer ausgewählt (siehe Abbildung 8-17). Diese Realisierung wird derzeit für den Einsatz in der Serienausstattung der Maschinen der Vollmer Werke Maschinenfabrik GmbH vorbereitet, da mit dieser Installation gleichzeitig ein wertvoller Zusatznutzen für die Kunden erzeugt werden kann (siehe Abschnitt 9.2, S. 224).

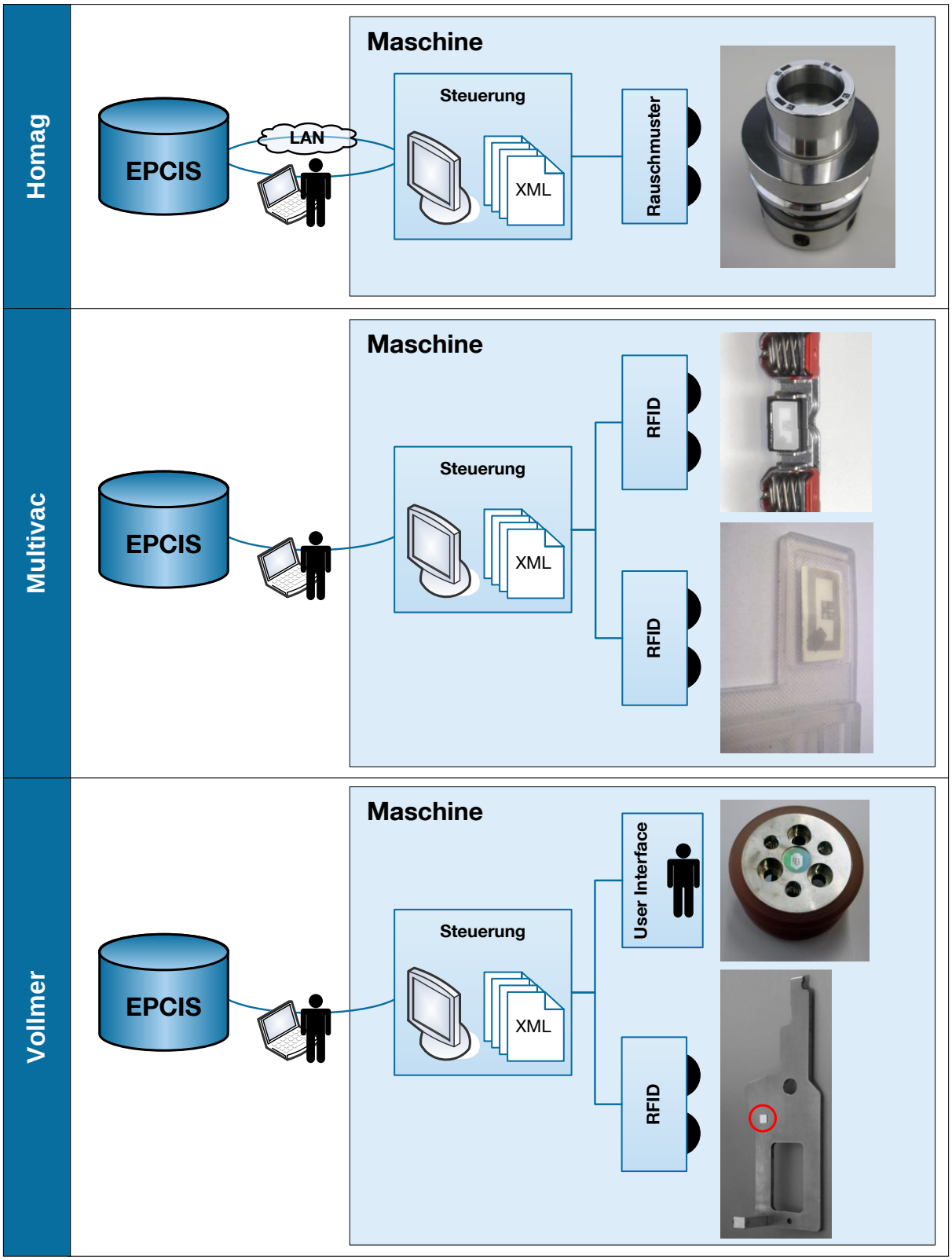


Abbildung 8-16: **Schematische Darstellung der Pilotinstallationen unter Verwendung der Symbolik aus Abbildung 8-2 (Bildquellen Bauteile: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, Vollmer Werke Maschinenfabrik GmbH)**

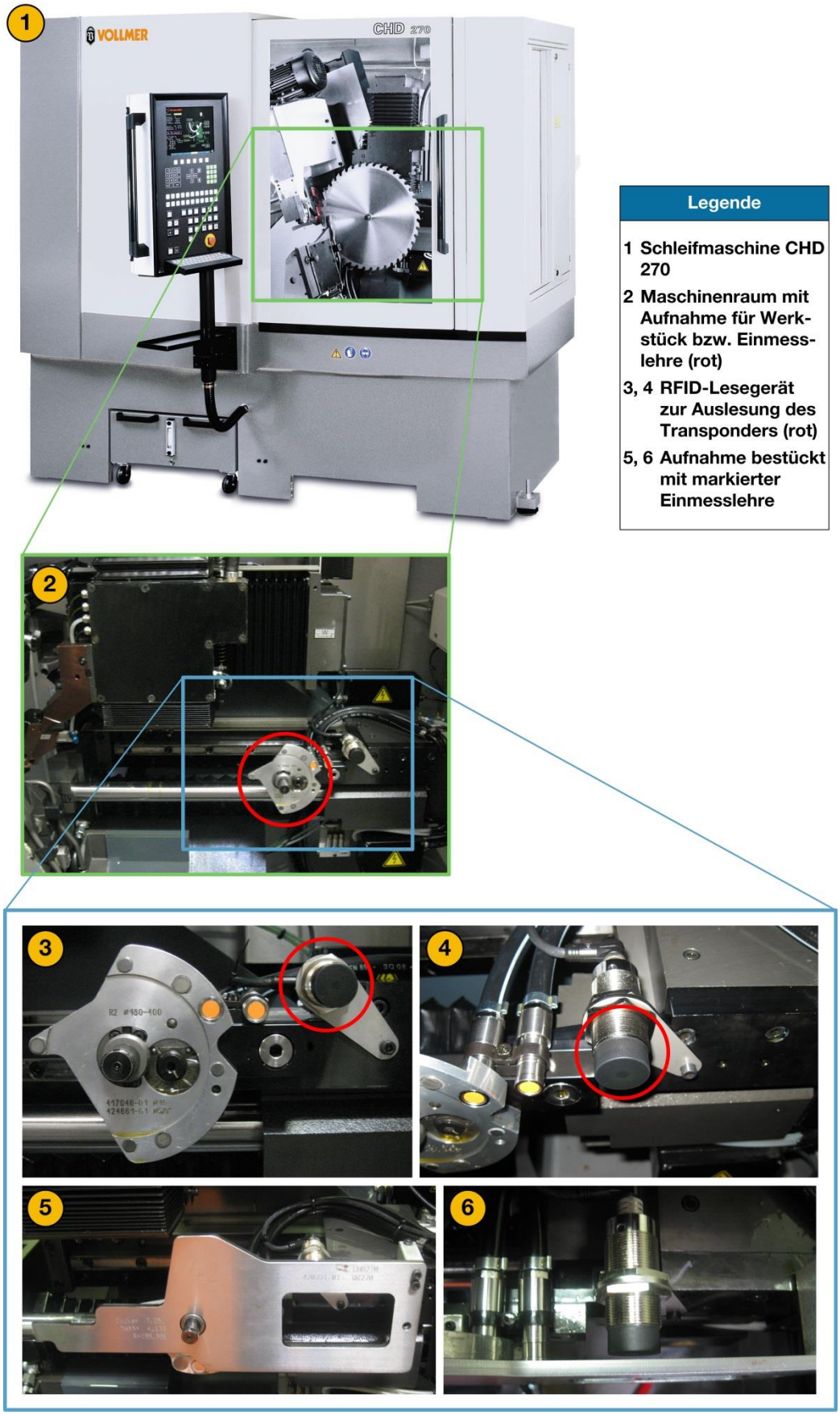


Abbildung 8-17: Reale Pilotinstallation am Beispiel der Einmesslehre von Vollmer (Bildquelle Maschine: Vollmer Werke Maschinenfabrik GmbH)

8.7 Ergebnisse und Abgleich mit den Anforderungen an das Produktpiraterie-Schutzsystem

In den Abschnitten 8.1 bis 8.6 wurde systematisch aufbauend aufgezeigt, wie das gesamte verteilte Produktpiraterie-Schutzsytem zur durchgängigen und dokumentierten Authentifizierung von Originalbauteilen konzipiert und ausgestaltet werden kann. Das Gesamtsystem schützt dabei die Supply-Chain sowie Maschinen und Anlagen. Es baut auf schützenswerten Bauteilen auf, welche ein Identitäts- und Sicherheitsmerkmal tragen, die gemäß dem Vorgehen in Kapitel 7, S. 105 ausgewählt und integriert wurden. Für das Produktpiraterie-Schutzsystem sind folgende Punkte berücksichtigt:

- Aufbau und Funktion von IP-Punkten in der Original-Supply-Chain sowie in Maschinen / Anlagen
- Aufbau eines Prüfdatensatzes mit Mindest- sowie optionalen Daten
- Modellierung der Datenweitergabe und -archivierung
- Möglichkeiten der Konsolidierung und Auswertung der Daten mit Visualisierungsvorschlägen
- Nutzung des Gesamtsystems bei Verwendung reiner Originalitätskennzeichen
- Implementierung des Produktpiraterie-Schutzsystems als Erweiterung des EPCglobal Network

Das Gesamtsystem wurde bereits in ersten Pilotinstallationen realisiert und seine Funktionen validiert. Die Berücksichtigung bzw. Abbildung der in Abschnitt 5.4, S. 95 formulierten Anforderungen an das Produktpiraterie-Schutzsystem werden in der folgenden Tabelle überprüft.

Tabelle 8-1: Abgleich Anforderungen

Nr.			Beschreibung
1			**Sicherheitsmerkmale**
			siehe Tabelle 7.10
2			**Anforderungen an ein System zur dokumentierten Authentifzierung**
	2.1		**Identifikations- und Prüfpunkte:**
		2.1.1 ✓	Integration beliebiger existierender oder neuer Sicherheitsmerkmale: Der aufgezeigte Aufbau ermöglicht es jederzeit, weitere Sicherheitsmerkmale zu qualifizieren und im Gesamtsystem zu integrieren (siehe Abschnitt 8.2). Dabei muss sichergestellt sein, dass die dort dargestellten Daten auch bei Verwendung einer neuen Technologie an einem IP-Punkt erzeugt werden können.
		2.1.2 ✓	Online- und Offline-Authentifizierung möglich: Durch die datentechnische Entkopplung der IP-Punkte vom gesamten verteilten Schutzsystem und lokale Authentifzierungsalgorithmen ist ein Offline-Betrieb jederzeit möglich (siehe Abschnitt 8.2). Alleine die Rückübertragung von gewonnenen Prüfdatensätzen für ein T&T sowie weitere Auswertungen sind in diesem Fall nur zeitverzögert möglich. Der einfachere Fall, dass ein IP-Punkt permanent online ist, ist ebenfalls im Gesamtsystem abgebildet.
		2.1.3 ✓	Unmittelbare Mitteilung des Prüfergebnisses an den Prüfer: Durch Verwendung lokaler Authentifizierungsalgorithmen bei IP-Punkten, die zeitweise offline sind, wird einem Prüfer das Prüfergebnis sofort am IP-Punkt angezeigt. Bei der Verwendung von Online-Prüfverfahren ist dies ebenso möglich - dabei muss natürlich sichergestellt sein, dass der IP-Punkt wirklich permanent eine Datenverbindung zum Authentifizierungssystem hat. (siehe Abschnitt 8.2)
		2.1.4	siehe Kapitel 9
		2.1.5 ✓	Lokale Speicherung des Prüfergebnisses zur Einsicht der Historie: Der Aufbau der IP-Punkte sieht explizit eine lokale Speicherung der Prüfdatensätze vor, um auch unabhängig von Datenbanken oder einer Zentralinstanz jederzeit Einblick in die lokale Prüfhistorie zu erlangen (siehe Abschnitt 8.2)
		2.1.6 ✓	Möglichkeit der Übertragung des Prüfergebnisses in eine zentrale Datenbank bei einer Freigabe durch den Maschinenbetreiber: Die Weitergabe der Daten ist im Gesamtsystem explizit vorgesehen und bei Verwendung derselben Datenbezeichner jederzeit korrekt interpretierbar (siehe Abschnitte 8.2, 8.3.1 und 8.4).
		2.1.7 ✓	IP-Punkte in einer Maschine / Anlage zur Authentifizierung eingebauter schützenswerter Bauteile in einer Maschine / Anlage beim Maschinenstart: Der Verbau und die steuerungstechnische Integration von IP-Punkten in Maschinen / Anlagen ist adressiert und abgebildet. Neben der konzeptionellen Darstellung in Abschnitt 8.3 sind Pilotrealisierungen in Abschnitt 8.6 benannt und abgebildet.
		2.1.8 ✓	Automatische, halbautomatische oder manuelle Authentifizierung eingebauter schützenswerter Bauteile: Dies ist rein vom verwendeten Sicherheitsmerkmal und der damit verbundenen Prüftechnologie abhängig. Für das Produktpiraterie-Schutzsystem ist lediglich wichtig, dass die an einem IP-Punkt erzeugten Daten für einen vollständigen Prüfdatensatz digital vorliegen (siehe Abschnitt 8.2). Die Erzeugung eines korrekten Prüfdatensatzes am IP-Punkt kann im einfachsten Fall vollautomatisch erfolgen, bei anderen Sicherheitsmerkmalen ist eine manuelle Unterstützung oder auch Dateneingabe erforderlich.
⋮			⋮

⋮			⋮
	2.2		**Gesamtsystem:**
		2.2.1 ✓	Beliebig viele Originalhersteller mit beliebig vielen Bauteilen und Komponenten: Das entwickelte verteilte Produktpirateriesschutzsystem kann beliebig viele Originalhersteller mit beliebig vielen Bauteilen und Komponenten abbilden, da beliebig viele Entitäten aufgenommen (siehe Abschnitt 8.3) und beliebig viele Teile mit entsprechenden Identitäts- und Sicherheitsmerkmalen ausgestattet werden können (siehe Abschnitt 8.1).
		2.2.2 ✓	Beliebig viele IP-Punkte in der originalen SC: Das entwickelte verteilte Produktpirateriesschutzsystem kann beliebig viele IP-Punkte abbilden, da beliebig viele Entitäten aufgenommen werden können (siehe Abschnitt 8.3).
		2.2.3 ✓	Möglichkeit der Datenübertragung der freigegebenen Daten in ein zentrales System: Dies ist im hier entwickelten Produktpirateriesschutzsystem explizit vorgesehen (siehe Abschnitt 8.3). Bei Verwendung des EPCglobal Network verbleiben die Daten in lokalen EPCIS-Repositories der einzelnen Beteiligten in der Supply-Chain. Bei der Auswertung der Daten wird dann - bei entsprechender Berechtigung - auf diese Daten lesend zugegriffen (siehe Abschnitt 8.4).
		2.2.4	siehe Kapitel 9
		2.2.5 ✓	Sicheres Hosting der Daten: Dies erfolgt gemäß dem Stand der Technik (siehe Abschnitt 3.2.1.3).
		2.2.6 ✓	Sicherer Datenaustausch: Dies erfolgt gemäß dem Stand der Technik (siehe Abschnitt 3.2.1.3).
	2.3 ✓		Datenmodell: Die einzelnen Prüfdatensätze müssen gewisse Mindestdaten beinhalten (siehe Abschnitt 8.2). Aber auch darüber hinausgehende Daten werden in den Beispielen der Prüfdatensätze dargestellt. Bei Verwendung des EPCglobal Networks ist der Datenaustausch auf Basis der darin definierten Bezeichner bereits standardisiert. Lediglich die neu hinzukommenden Argumente müssten für einen reibungslosen Datenaustausch einheitlich benannt sein (siehe Abschnitt 8.4).
	2.4		**Auswertung:**
		2.4.1 ✓	Zusammenführung, Auswertung und Ausgabe der freigegebenen Daten zu einer Originalware: Dies ist in der vorgestellten Architektur jederzeit möglich (siehe Abschnitt 8.3). Ein Vorschlag zur Visualisierung der T&T- in Kombination mit den Authentifizierungs-informationen für sowohl Unikatkennzeichen als auch reine Originalitätskennzeichen ist in den Abschnitten 8.4 und 8.5 dargestellt. Im EPCglobal Network sind entsprechende Auswertungen ebenfalls vorgesehen (siehe Abschnitt 8.4).
		2.4.2 ✓	Zusammenführung, Auswertung und Ausgabe der freigegebenen Daten zu einer Maschine: Dies ist in der vorgestellten Architektur dadurch jederzeit möglich, dass in den Maschinen / Anlagen integrierte IP-Punkte ebenso zum Gesamtsystem gehören (siehe Abschnitt 8.3). Dasselbe gilt für die Verwendung des EPCglobal Network (siehe Abschnitt 8.4).
		2.4.3	siehe Kapitel 9

9 Systemreaktionen und Zusatznutzen

Nach der Beschreibung der Systemarchitektur für das verteilte Produktpiraterie-Schutzsystem werden in diesem Kapitel Möglichkeiten aufgezeigt, wie auf Prüfergebnisse reagiert und wie mittels neuer, passender Zusatznutzen eine Win-win-Situation für alle Wirtschaftsbeteiligten erzeugt werden kann. Im strategischen Vorgehen in Abbildung 5-6, S. 92 entspricht dies dem letzten „Schritt 5“.

9.1 Systemreaktionen

Die Systemreaktionen im Produktpiraterie-Schutzsystem sind in erster Linie vom Authentifizierungsergebnis bei einer Bauteilüberprüfung an einem IP-Punkt abhängig. Das Prüfergebnis kann zwei Ausprägungen haben: „Original“ oder „Kann nicht als Original bestätigt werden“ (siehe Abschnitt 7.4.2, S. 164 sowie Abbildung 8-12, S. 202 und Abbildung 8-15, S. 207). Des Weiteren ist die Systemreaktion davon abhängig, ob diese lokal, also am IP-Punkt selbst oder aufgrund von Erkenntnissen in der Gesamtsicht aller Daten und somit zentral seitens des Originalherstellers erfolgen soll. Ein weiterer Gesichtspunkt ist der zeitliche Bezug – soll das System zeitlich unmittelbar auf ein Prüfergebnis reagieren oder ist eine zeitlich verzögerte Reaktion sinnvoll oder aus technisch-organisatorischen Gründen nur in dieser Form möglich.

In Tabelle 9-1 sind die Möglichkeiten als Übersicht aufgezeigt und in den Abschnitten 9.1.1 und 9.1.2 gemäß der Nummerierung beschrieben. Dabei ist festzustellen, dass eine verzögerte Systemreaktion am IP-Punkt in der Supply-Chain keinen Sinn ergibt. Andererseits ist eine sofortige Reaktion beim Hersteller aus technisch-organisatorischer Sicht schwer realisierbar und ebenfalls nicht sinnvoll. Beide Fälle sind daher in Tabelle 9-1 nicht beinhaltet.

Tabelle 9-1: Kategorisierung möglicher Systemreaktionen

Systemischer Ansatz	Lokal			Zentral
Ort	IP-Punkt in der Supply-Chain	IP-Punkt in der Maschine		Original-hersteller
Zeitlicher Bezug	sofort	sofort	verzögert / bei Bedarf	verzögert / bei Bedarf
Original	L.1	L.3	L.5	Z.1
Keine korrekte Authentifizierung	L.2	L.4	L.6	Z.2

9.1.1 Systemreaktion lokal

L.1 Original: Lokale, sofortige Systemreaktion am IP-Punkt in der Supply-Chain

Wie bereits in Abschnitt 8.2, S. 181 dargestellt, ist eine sofortige Anzeige des Authentifizierungsergebnisses am IP-Punkt für den Nutzer sehr wichtig. So kann dieser unmittelbar auf das Prüfergebnis reagieren. Dabei sollte das positive Prüfergebnis, dass ein Original vorliegt, entsprechend textlich dargestellt und farblich visualisiert werden. In einer Erstrealisierung wurden dafür die Argumente des Datensatzes verwendet und angezeigt sowie der gesamte Datensatz sinnfällig farblich grün hinterlegt – das visuelle Signal, dass das vorliegende Bauteil ein Original darstellt (siehe Abbildung 9-1). In diesem Fall bleibt das Argument „Maschinennummer“ frei, da das Bauteil noch nicht verbaut ist. Zusätzlich wird der gesamte Datensatz lokal am IP-Punkt gespeichert und bei bestehender Freigabe in ein Datenarchivierungs- und -auswertesystem übertragen (siehe Abschnitte 8.2, S. 181 und 8.3, S. 188).

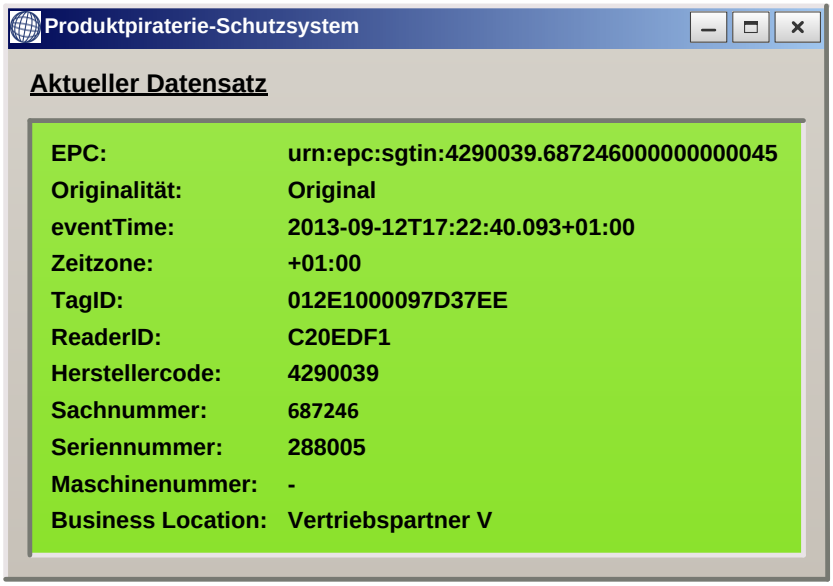


Abbildung 9-1: Visualisierung des Prüfdatensatzes für das zuletzt geprüfte Originalbauteil an einem IP-Punkt in der Supply-Chain

L.2 Keine korrekte Authentifizierung: Lokale, sofortige Systemreaktion am IP-Punkt in der Supply-Chain

Analog zu der Darstellung in L.1 werden im Falle einer nicht korrekten Authentifizierung alle Argumente des Datensatzes angezeigt. Es erfolgt die textliche Mitteilung, dass das vorliegende Bauteil nicht als Original authentifiziert werden konnte und der gesamte Datensatz wird sinnfällig farblich rot hinterlegt – das visuelle Signal, dass das vorliegende Bauteil kein Original ist (siehe Abbildung 9-2). Auch hier bleibt das Argument „Maschinennummer“ frei, da das Bauteil noch nicht verbaut ist. Zusätzlich wird der gesamte Datensatz lokal am IP-Punkt gespeichert und bei bestehender Freigabe in ein Datenarchivierungs- und -auswertesystem übertragen (siehe Abschnitte 8.2, S. 181 und 8.3, S. 188).

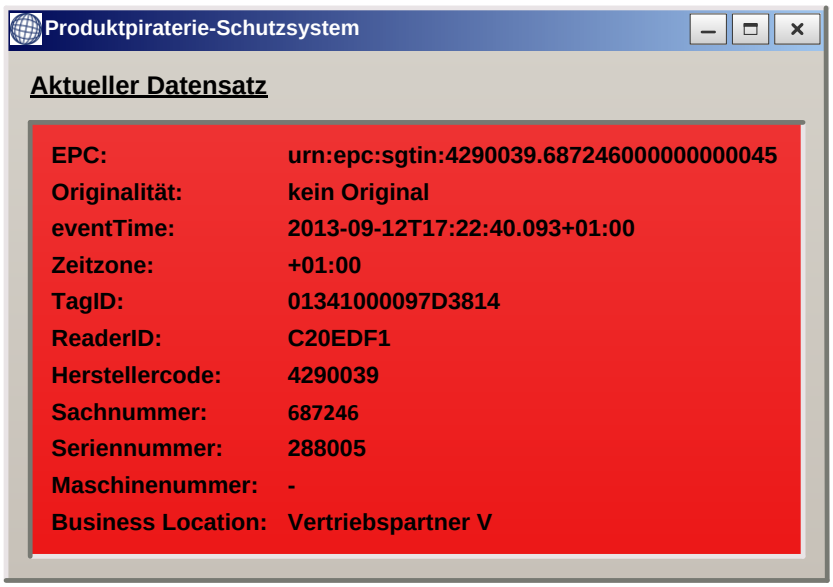


Abbildung 9-2: Visualisierung des Prüfdatensatzes für das zuletzt geprüfte nicht-originale Bauteil an einem IP-Punkt in der Supply-Chain

L.3 Original: Lokale, sofortige Systemreaktion am IP-Punkt in der Maschine

Analog zu den Prüfungen in der Supply-Chain (siehe Punkte L.1 und L.2) soll auch am IP-Punkt in der Maschine eine sofortige Anzeige der Prüfergebnisse stattfinden. Die Form der Darstellung ist dabei sicherlich von der Anzahl der überprüften Bauteile abhängig. Sollte es sich lediglich um ein einzelnes Bauteil handeln, könnte die Visualisierung an der Benutzerschnittstelle analog zu den vorangegangenen Visualisierungen in der Supply-Chain gestaltet werden und ist bzgl. des Arguments „Maschinennummer“ vollständig. Zusätzlich ist in Abbildung 9-3 ein Hinweis für den Maschinenbediener dargestellt, der nur erscheint, wenn alle geprüften Bauteile Originale sind. Wie in den vorangegangenen IP-Punkten in der Supply-Chain wird auch hier der gesamte Datensatz lokal am IP-Punkt gespeichert und bei bestehender Freigabe in ein Datenarchivierungs- und -auswertesystem übertragen (siehe Abschnitte 8.2, S. 181 und 8.3, S. 188).

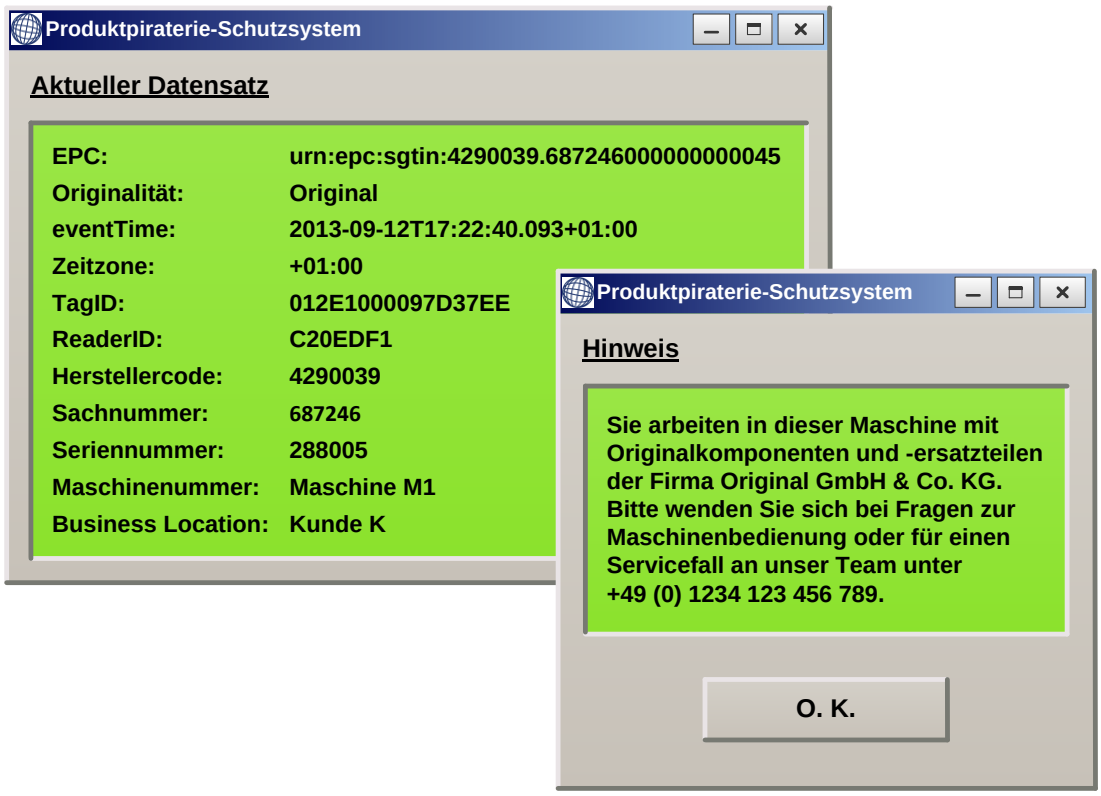


Abbildung 9-3: Visualisierung des Prüfdatensatzes und eines Hinweises für den Maschinenbediener für das geprüfte Originalbauteil an der Maschine M1 direkt nach dem Maschinenstart

L.4 Keine korrekte Authentifizierung: Lokale, sofortige Systemreaktion am IP-Punkt in der Maschine

Dieser Fall ist einer der kritischsten im gesamten Produktpiraterie-Schutzsystem: die Verwendung von nicht-originalen Bauteilen auf Maschinen oder Anlagen. Die Schwierigkeit liegt im Bereich der juristischen Folgen, die daraus erwachsen können und die immer fallspezifisch juristisch zu bewerten sind. Bei der Verwendung von Komponenten und Ersatzteilen, die kein Original sind, sowie bei etwaigen Reaktionen des Produktpiraterie-Schutzsystems an Maschinen / Anlagen können folgende rechtliche Konfliktbereiche berührt sein [Ben-10 S. 131 ff., Gün-11b, Pro-09 S. 34]:

- Gewährleistungsrecht nach dem Bürgerlichen Gesetzbuch (BGB), insbesondere § 437 und § 634 BGB, bspw. Kostenübernahmeansprüche aus Instandsetzung aufgrund eines Mangels [BMJ-13d]
- Gesetz über die Haftung für fehlerhafte Produkte (ProdHaftG), bspw. Schadensersatzansprüche aufgrund von durch eine Maschine verursachter Schäden [BMJ-13c]

- Kartellrecht nach Artikel 101 und Artikel 102 des Vertrags über die Arbeitsweise der Europäischen Union, bspw. bezüglich Wettbewerbsbeschränkungen bei vertraglich geregelten Alleinbezugsverpflichtungen [Amt-12]
- Gesetz gegen Wettbewerbsbeschränkungen (GWB), bspw. bezüglich Wettbewerbsbeschränkungen bei vertraglich geregelten Alleinbezugsverpflichtungen [BMJ-13a]
- Gesetz gegen den unlauteren Wettbewerb (UWG), bspw. bei Irreführung und Täuschung von Kunden [BMJ-13b]
- Vertragsrecht nach dem Bürgerlichen Gesetzbuch (BGB), bspw. aufgrund einer vertraglich vereinbarten Maschinenverfügbarkeit [BMJ-13d]
- Eigentumsrechte nach § 903 BGB [BMJ-13d]
- Allgemeine Geschäftsbedingungen (AGB), bspw. bei Garantiezusagen

Um bei lokalen Reaktionen der Maschine auf Bauteile, die nicht authentifiziert werden können, nicht in Konflikt mit einem der genannten rechtlichen Bereiche zu geraten, sollte vor Einführung einer solchen Reaktion immer der spezifische Fall überprüft werden. Negative Reaktionen auf nicht-authentifizierte Bauteile, welche Einfluss auf die Leistung der Maschine nehmen, verstoßen z. B. gegen das GWB. Eine Maschinenstilllegung könnte z. B. in das Eigentum des Inhabers eingreifen. Daher sind in diesem Fall neutrale Reaktionen sinnvoll, beispielsweise Hinweise ohne oder auch mit Bestätigungserfordernis.

Wie eine solche Information aussehen könnte, ist in Abbildung 9-4 zu sehen, die aber für konkrete Fälle auf ihre rechtliche Korrektheit zu prüfen ist. Zusätzlich zu dieser Information an der Benutzerschnittstelle wird der gesamte Datensatz lokal am IP-Punkt gespeichert und bei bestehender Freigabe in ein Datenarchivierungs- und -auswertesystem übertragen (siehe Abschnitte 8.2, S. 181 und 8.3, S. 188).

Die Wirkung des Schutzkonzepts ist somit klar darauf ausgerichtet, eine überwachende und beweissichernde Funktion auszuführen. Es geht insbesondere nicht um die Beschränkung des Wettbewerbs o. Ä. Die Verwendung der Kennzeichnungstechnologien im Kontext des gesamten Produktpiraterie-Schutzsystems ermöglicht es dem Originalhersteller, den Nachweis von Vertragsverstößen und den Schutz vor unberechtigten Ansprüchen, bspw. für durch Fremdbauteile entstandene Schäden, zu erbringen. [Ben-10 S. 131 ff., Gün-11b]

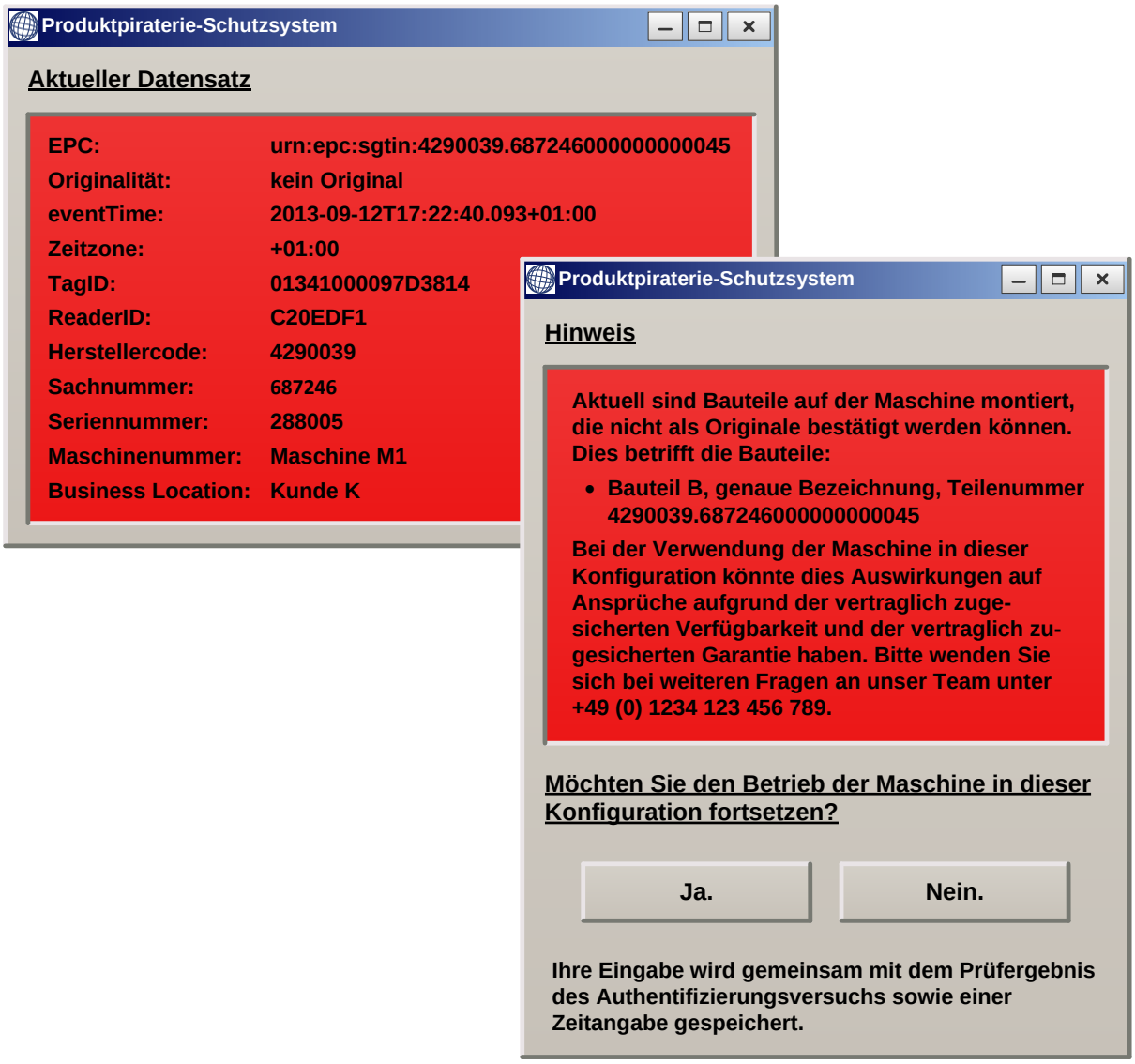


Abbildung 9-4: Visualisierung des Prüfdatensatzes und eines Hinweises für den Maschinenbediener für das geprüfte nicht-originale Bauteil an der Maschine M1 direkt nach dem Maschinenneustart

L.5 Original: Lokale, bedarfsabhängige Systemreaktion am IP-Punkt in der Maschine

Dieser Fall bezieht sich beispielsweise auf die Überprüfung der Maschine durch einen Servicetechniker des Originalherstellers vor Ort bei einem Gewährleistungsfall. Sofern dabei lediglich Originalteile auf der Maschine montiert sind und die Einsichtnahme der Prüfhistorie an der Maschine ebenso nur die Verwendung von Originalbauteilen aufzeigt, muss der Originalhersteller die Kosten für die Instandsetzung übernehmen. In diesem Fall erfolgt somit keine besondere Reaktion.

L.6 Keine korrekte Authentifizierung:
Lokale, bedarfsabhängige Systemreaktion am IP-Punkt in der Maschine

Dieser Fall bezieht sich beispielsweise auf die Überprüfung der Maschine durch einen Servicetechniker des Originalherstellers vor Ort bei einem Gewährleistungsfall, wie dieser auch in L.5 dargestellt wurde. Hier ist allerdings der Unterschied, dass Bauteile, die entweder aktuell auf der Maschine montiert sind oder in der Vergangenheit verwendet wurden, nicht als Originale bestätigt werden konnten. In diesem Fall müsste der Servicetechniker an den Maschinenbetreiber den Hinweis geben, dass die Instandsetzung fortgesetzt werden kann, die Kostenübernahme jedoch im Nachgang zu klären ist.

9.1.2 Systemreaktion zentral

Auswertungen der zentral zusammengeführten Daten können die in Abschnitt 8.4.2.1 und 8.5 aufgezeigten Abfragen mit den in Abbildung 8-12 und Abbildung 8-15 schematisch dargestellten Visualisierungen beantworten (siehe S. 202 und 207). Dabei stellt sich die Frage, wie mit den Auswerteergebnissen beim Originalhersteller umgegangen werden kann.

Z.1 Original:
Zentrale, bedarfsabhängige Systemreaktion beim Originalhersteller

In dem Fall, dass innerhalb einer Supply-Chain keine Unregelmäßigkeiten festgestellt werden können, gibt es keine besondere Reaktion seitens des Originalherstellers. Sollte dies bei einer konkreten Maschine festgestellt werden, ist dies sehr erfreulich und der Originalhersteller könnte mit einem Belohnungs- / Bonussystem arbeiten (siehe Abschnitt 9.2).

Z.2 Keine korrekte Authentifizierung:
Zentrale, bedarfsabhängige Systemreaktion beim Originalhersteller

In dem Fall, dass zu gewissen Zeitpunkten an bestimmten Orten in der Supply-Chain oder in einer Maschine keine Originalbauteile erkannt werden konnten, ist eine Reaktion seitens des Originalherstellers notwendig. Handelt es sich um Vorfälle in der Supply-Chain, ist eine Klärung des Sachverhalts zusammen mit dem betreffenden Partner zielführend (siehe Warenausgang des Logistikdienstleisters in Abbildung 8-15, S. 207).

Bei Vorfällen mit Verwendung von nicht-originalen Bauteilen auf Maschinen / Anlagen des Originalherstellers (siehe Abbildung 8-12, S. 202, Bauteil 4 oder Abbildung 8-15, S. 207 mit Maschine M1 bzw. M2) kann ebenso mit klärenden Gesprächen gearbeitet werden. Die Firma Müller Martini GmbH hat mit dieser aktiven Vorgehensweise sehr gute Erfahrungen mit ihren Kunden gemacht, die sehr offen Rückmeldung auf die Fragen der Vertriebsexperten bezüglich ihrer Gründe und Motivation gegeben haben [Ben-12]. Eine starke Weiterentwicklung der Vertriebsaktivitäten im After-Sales-Geschäft ist somit gegeben, was sich im stark steigenden Umsatz im After-Sales, neuen Service-Angeboten und sogar in einem neuen Preis-Modell für Ersatzteile von Müller Martini ausdrückt [Ben-10 S. 143ff., Ben-13, Mül-13]. Möglichkeiten und Argumente, Kunden zurückzugewinnen, bieten dabei auch die in Abschnitt 9.2 dargestellten Zusatznutzen.

Die Erkenntnis und Dokumentation, dass in bestimmten Maschinen / Anlagen Bauteile verwendet werden, die nicht als Originale authentifiziert werden können, ist jedoch sicherlich auch im Falle von Gewährleistungsanfragen, Garantieanfragen, Ansprüchen aus nicht erfüllten vertraglichen Zusicherungen (z. B. Maschinenverfügbarkeit), etc. von zentraler Bedeutung, um mit diesen Fällen passend umgehen zu können.

9.1.3 Einordnung der Systemreaktionen

Um das gesamte Produktpiraterie-Schutzsystem sinnvoll und insbesondere mit allen Funktionsmöglichkeiten einzusetzen, sind die Systemreaktionen sicherlich eine sehr wichtige Komponente. Einerseits bleibt der Originalhersteller mit entsprechend visualisierten Mitteilungen an den Benutzerschnittstellen der IP-Punkte mit den Beteiligten der Supply-Chain in Kontakt, andererseits kann das Gesamtsystem bei der Auswertung der gesammelten Daten aus dem Feld positiv wirken, wenn dabei erkennbare Nutzen für den Kunden entstehen. Dies wird mit den Zusatznutzen im nächsten Abschnitt dargestellt.

9.2 Zusatznutzen

Das entwickelte Produktpiraterie-Schutzsystem dient bisher rein der Überwachung des gesamten Logistiknetzwerks der Originalhersteller im Maschinen- und Anlagenbau sowie deren Maschinen / Anlagen. Dabei können für die schützenswerten und markierten Bauteile T&T-Daten gemeinsam mit den Prüfergebnissen der Authentifizierungen im gesamten Netzwerk ausgetauscht werden (siehe Kapitel 8, S. 179).

Um das Gesamtsystem über diese Funktionen hinaus für alle Wirtschaftsbeteiligten des Wertschöpfungs- und Logistiknetzwerks attraktiv zu gestalten und damit wirtschaftlicher zu machen, können auf dem vorgestellten verteilten IT-System weitere Funktionen, sogenannte Zusatznutzen, implementiert werden. Die Definition von Zusatznutzen ist wie folgt:

> Zusatznutzen:
> Unter einem Zusatznutzen wird eine Systemfunktion verstanden, die über die reine Kennzeichnung und Authentifizierung sowie deren Ergebnisanzeige und -dokumentation hinausgeht. [Gün-11c]

Diese Zusatznutzen stellen damit einen Mehrwert für den Originalhersteller, den Maschinenbetreiber als Kunde oder weitere Beteiligte der Supply-Chain, die einen IP-Punkt (siehe Abschnitt 8.2, S. 181) betreiben, dar. Gemäß dieser Definition ist die Zusammenführung und Visualisierung der T&T-Daten über einzelne Bauteile sowie der aktuellen Maschinenkonfiguration der erste mögliche Zusatznutzen (siehe Abbildung 8-12, S. 202 und Abbildung 8-15, S. 207). Weitere im Forschungsprojekt identifizierte und mit dem Produktpiraterie-Schutzsystem verknüpf- bzw. realisierbare Zusatznutzen sind in Tabelle 9-2 und Tabelle 9-3 gelistet. Die Zusatznutzen können eingeteilt werden in lokale Zusatznutzen an einem Bauteil oder an einer Maschine / Anlage, sowie in zentrale Zusatznutzen, die aufgrund der zentralen Sicht auf die gesammelten Daten oder aus der Position des Originalherstellers möglich sind.

9.2.1 Lokale Zusatznutzen

Tabelle 9-2: Lokal an einem Bauteil oder einer Maschine zu realisierende Zusatznutzen, in Anlehnung an die Vorveröffentlichung des Autors in [Gün-11c]

Sicherheitsmerkmal am Bauteil	Funktionen an der Maschine / Anlage
• Steigerung der Qualitätsanmutung • Gütesiegel • Gerichtsverwertbarkeit	• Automatische Bauteil- / Werkzeugidentifikation ermöglicht: ○ Verwechslungsschutz für Bauteile / Werkzeuge ○ Automatische Datenübergabe bauteil- oder werkzeugindividueller Betriebsparameter ○ Selbstkonfiguration der Gesamtmaschine bei Verwendung von Originalbauteilen • Erstellung sowie automatische Aktualisierung einer der Realität entsprechenden Maschinenstückliste / -konfiguration • Bauteilindividuelle Standzeiterfassung oder Protokollierung der Taktzeit / Zyklen des Bauteils als Betriebsdatenerfassung (BDE) ermöglicht: ○ Unterstützung des Condition-Monitoring ○ Verschleißprognose, dargestellt in einer Serviceampel zur Anzeige der nächsten notwendigen Wartung

Insbesondere die als Zusatznutzen genannten Funktionen an der Maschine / Anlage sind für den Kunden sehr interessant, da dadurch die Möglichkeit eröffnet wird, bei Verwendung von Originalbauteilen in der Produktion einerseits direkt Zeit einzusparen, andererseits die Produktionssicherheit zu erhöhen. Bei automatischer Neukonfiguration der Maschinenbetriebsparameter bei Erkennung von markierten Bauteilen beschleunigt das den Einrichtprozess einer Maschine deutlich, der manuelle Aufwand zur Einstellung einer Maschine wird reduziert oder entfällt komplett.

Die Verschleißprognose für Originalbauteile hilft, eine bislang zyklische Wartung einer Maschine in eine bedarfsgesteuerte Wartung zu überführen. Diese Verschleißprognose erfolgt über eine Analyse der erfassten Standzeit aller Originalbauteile im Feld. Diese Größe lässt sich aus den im Produktpiraterie-Schutzsystem erfassten

Authentifizierungsdaten (siehe Abbildung 8-3, S. 184) ableiten und kommt dem einzelnen Kunden an seiner Maschine lokal zugute.

9.2.2 Zentrale Zusatznutzen

Bei den zentralen Zusatznutzen ist sicherlich zunächst der wichtigste Zusatznutzen anzuführen: Das T&T für Ersatzteile und Komponenten des Originalherstellers. Damit können die Bauteile auf ihrem Weg durch das Logistiknetzwerk verfolgt und rückverfolgt werden. Dieser und weitere Zusatznutzen sind in Tabelle 9-3 zusammengefasst und eingeordnet.

Tabelle 9-3: Zentral im System zu realisierende Zusatznutzen, in Anlehnung an die Vorveröffentlichung des Autors in [Gün-11c]

Ersatzteil-management	Service	Betriebswirtschaft und Marketing
• Erleichterte Ersatzteilbeschaffung mit sicherer Bestellung und Lieferung, da Verwechslungen aufgrund eindeutiger Bauteilkennzeichnungen ausgeschlossen sind • Nachverfolgbarkeit der Ersatzteile auf dem Transportweg • Ermittlung von Felddaten, z. B. für die Prognose des Verschleißes von Originalbauteilen • Reduzierung der Lagerkosten durch optimales Ersatzteilmanagement auf Basis von Verschleißprognosen	• Optimale Vorbereitung der Servicetechniker durch genaue Kenntnis der realen Maschinenkonfiguration • Neue Fernwartungskonzepte verbunden mit den Unikatkennzeichen der Originalteile • Längere Wartungsintervalle als Folge der Verschleißprognose, nur bei Originalbauteilen möglich • Gewährung einer Garantie über die Gewährleistung hinaus bei Verwendung von Originalbauteilen • Erleichterte Rückrufaktion	• Klassifizierung der Kunden und individuelles Marketing • Vergünstigungen in Wartungsverträgen für treue Kunden • Bonusprogramme / Rabatte für nachweislich treue Kunden • Abwrackprämie und Recycling für alle Bauteile (auch Nicht-Originale) mit dem Ziel der Feststellung der Haltbarkeit des Originals im Vergleich zur Kopie und damit deren Wirtschaftlichkeit • Meldung an lokalen Vertriebspartner bei Einsatz von Kopien für gezieltes Marketing

Im Bereich des Ersatzteilmanagements liegt der Zusatznutzen im Bereich der Bauteile selbst und hat einen starken Bezug zu den Teilen. Gerade die Ermittlung von Felddaten dürfte für den Originalhersteller äußerst wertvoll einerseits für die Argumentation für die Verwendung von Originalbauteilen sein, andererseits für die Entwicklung, um Stärken und Schwächen der eigenen Bauteile besser einschätzen zu können. Von besonderem Interesse ist dabei die Authentifizierung am IP-Punkt in Maschinen. Bei jeder Authentifizierung wird dabei ein Datensatz mit Zeitstempel erzeugt. Die Auswertung aller Datensätze über die im Feld befindlichen Teile einer

Sachnummer lässt die Ermittlung der Standzeit und somit zukünftig deren Prognose zu.

In den Bereichen „Service“ und „Betriebswirtschaft und Marketing“ entfernen sich die Zusatznutzen immer weiter vom technischen System, ergänzen jedoch die Kennzeichnung und Authentifizierung zu einem runden Gesamtsystem. Dabei liefert beispielsweise der Vergleich zwischen Originalbauteilen und Kopien eine wertvolle Argumentationsbasis für das Marketing und den Vertrieb im After-Sales-Geschäft. Dies wird zusätzlich durch die Kennzeichnung und eindeutige Unterscheidbarkeit der Originale von Kopien unterstützt. Eine Abwrackprämie für alle Komponenten und Ersatzteile – unabhängig von deren Herkunft – ermöglicht es, diese Bauteile zu bekommen und bewerten zu können. Bei der Bildung von Kundenklassen und dem Einsatz von Bonussystemen wäre denkbar:

- Verkürzte Reaktionszeit im Servicefall für einen Premiumkunden, der nur Originalbauteile verwendet, bis hin zu einem Just-in-time-Servicemitarbeiter bei Kombination mit einer Verschleißprognose
- Zugang zu exklusiven Informationen und Veranstaltungen wie z. B. die Einladung zu Produktpräsentationen für Premiumkunden

9.3 Beispiele: Realisierung vom Zusatznutzen

Die Möglichkeiten, mit dem Produktpiraterie-Schutzsystem gleichzeitig weitere Funktionen in Form von Zusatznutzen zu implementieren, macht das gesamte Produktpiraterie-Schutzsystem für alle Beteiligten des Logistiknetzwerks attraktiv. Am Beispiel der Vollmer Werke Maschinenfabrik GmbH soll hier aufgezeigt werden, wie Zusatznutzen sinnvoll integriert werden können. Dabei werden die Beispiele aus den Abschnitten 5.2.2, 7.1.3, 7.2.3, 7.5.2 und 8.6 (S. 89, 121, 157, 175 und 207) hier fortgesetzt.

9.3.1 Drahttransportrolle der Vollmer Werke Maschinenfabrik GmbH

Die Drahttransportrolle ist ein, von außen sichtbares Bauteil an Drahterodiermaschinen der Firma Vollmer. Das Hologramm als Sicherheitsmerkmal (siehe Abschnitte 7.1.3, 7.2.3, 7.5.2 und 8.6 auf S. 121, 157, 175 und 207) erhöht die Qualitätsanmutung des Originalbauteils und ist zudem von jedem Maschinenbediener sofort einsehbar (Abbildung 9-5).

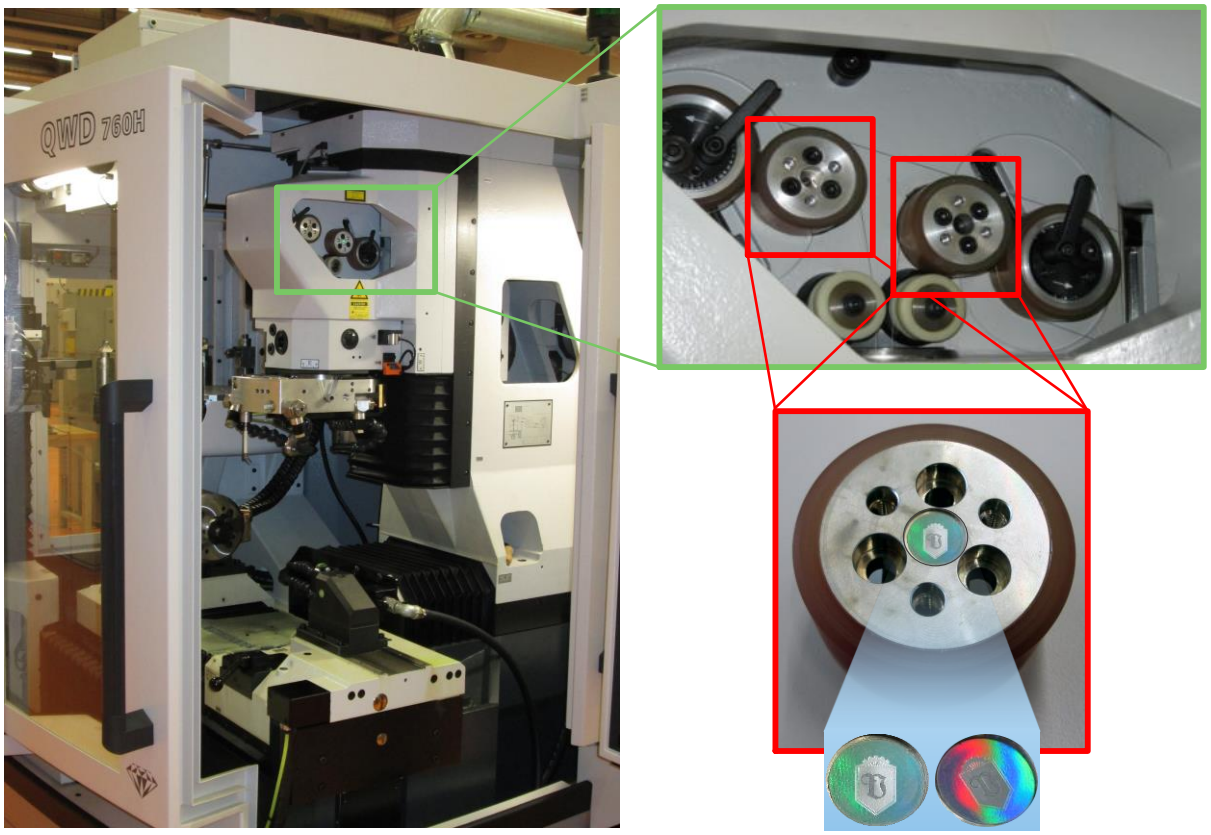


Abbildung 9-5: Zusatznutzen „Qualitätsanmutung“ bei der Drahttransportrolle (Bildquelle Maschine / Bauteil: Vollmer Werke Maschinenfabrik GmbH)

9.3.2 Einmesslehre der Vollmer Werke Maschinenfabrik GmbH

Bei der Einmesslehre wird RFID als Sicherheitsmerkmal eingesetzt (siehe Abschnitte 7.1.3, 7.2.3, 7.5.2 und 8.6 auf S. 121, 157, 175 und 207). Neben den Identifikations- und Authentifizierungsdaten werden auch spezifische Maße der jeweiligen Einmesslehre im Transponder abgespeichert (siehe Abbildung 9-6):

- Dicke (z. B. 7,410 mm)
- Maß X (z. B. 3,976 mm)
- Radius (z. B. 200,002 mm)

Diese Maße werden bei der Kalibrierung einer Maschine benötigt. Eine Falscheingabe führt zu Fehleinstellungen oder sogar zum Maschinencrash. Daher wird der Maschinenbediener mit Hilfe des IP-Punktes in der Maschine unterstützt.

Bei der Authentifizierung der Einmesslehre werden diese drei Maße an die Maschine automatisch übergeben und liegen somit für den Kalibrierungslauf vor (siehe Abbildung 8-17, S. 210). Eine manuelle Eingabe ist damit nicht mehr notwendig und der

Prozess insgesamt beschleunigt. Die Sicherheit wird zusätzlich erhöht, weil Falscheingaben ausgeschlossen sind. Damit sind die folgenden Zusatznutzen umgesetzt:

- Automatische Bauteil- / Werkzeugidentifikation
- Automatische Datenübergabe spezifischer Parameter
- Selbstkonfiguration der Gesamtmaschine bei Verwendung von Originalbauteilen

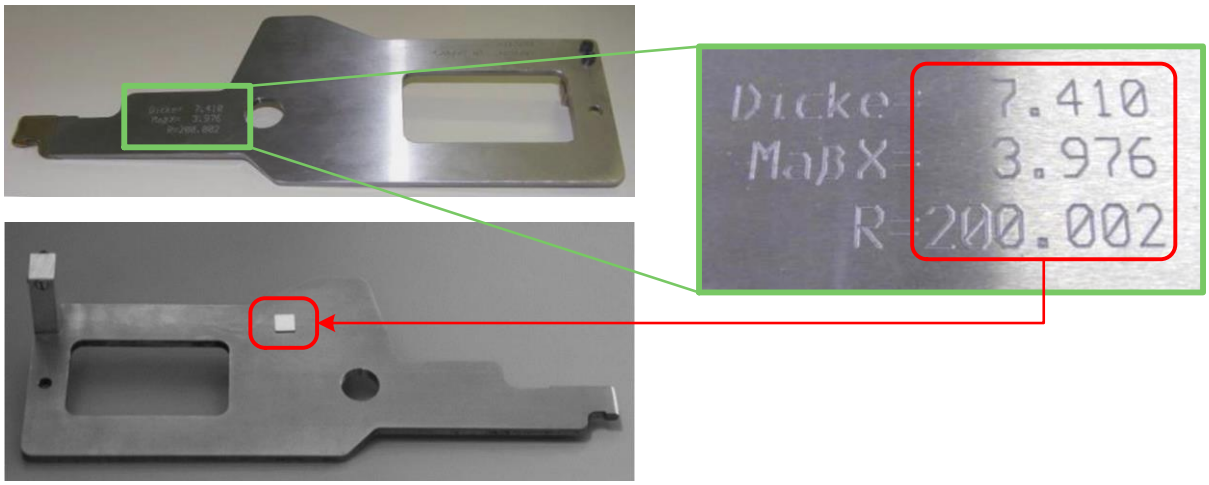


Abbildung 9-6: Zusatznutzen „Automatische Bauteil- / Werkzeugidentifikation“, „Automatische Datenübergabe spezifischer Parameter“ sowie „Selbstkonfiguration der Gesamtmaschine bei Verwendung von Originalbauteilen“ bei der Einmesslehre (Bildquelle Bauteil: Vollmer Werke Maschinenfabrik GmbH)

9.4 Rechtliche Zulässigkeit des entwickelten technischen Produktpiraterie-Schutzsystems

Das gesamte entwickelte und in den Kapiteln fünf bis neun systematisch aufbauend dargestellte Produktpiraterie-Schutzsystem konnte bereits von der juristischen Seite abgesichert werden. Der Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum der Technischen Universität München hat bei der Prüfung des Gesamtsystems folgendes Ergebnis erarbeitet [Gün-11c S. 44]:

- „Prinzipiell ist das Prüfen von Bauteilen und deren Originalität in Maschinen mit überwachender und beweissichernder Funktion möglich, um ungerechtfertigte Gewährleistungsansprüche abwehren zu können.“
- „Die Übertragung der gewonnenen Daten in ein zentrales System muss zwischen Maschinenhersteller und Maschinenkäufer / -betreiber vertraglich klar geregelt sein.“

- „Als zusätzliche Maßnahme können zwischen dem Originalhersteller und dem Maschinenkäufer / -betreiber Alleinbezugsvereinbarungen vereinbart werden, wobei das Wettbewerbsrecht und das AGB-Recht berücksichtigt werden müssen, vor allem bezüglich der gegenständlichen und zeitlichen Höchstdauer der Bindung.“ [34]

9.5 Zusammenfassung und Abgleich mit den Anforderungen an das Produktpiraterie-Schutzsystem

In den Abschnitten 9.1 bis 9.3 wurde dargestellt, welche Reaktionen im verteilten Produktpiraterie-Schutzsystem einerseits lokal an den IP-Punkten oder auch zentral aus der Analyse der Gesamtdaten durch den Originalhersteller erfolgen können. Zudem wurde aufgezeigt, welche Zusatznutzen, die über die reine Authentifizierung sowie deren Ergebnisanzeige und -dokumentation hinausgehen, im Forschungsprojekt identifiziert wurden und mit diesem System verknüpfbar sind, um eine Win-win-Situation für alle Beteiligten des Wertschöpfungs- und Logistiknetzwerks zu schaffen. Auch wurde, wie in Abschnitt 9.4 dargestellt, das gesamte entwickelte Produktpiraterie-Schutzsystem bereits von juristischer Seite abgesichert und unter den genannten Voraussetzungen als zulässig eingestuft.

Die Berücksichtigung bzw. Abbildung der in Abschnitt 5.4, S. 95 formulierten Anforderungen an die Systemreaktionen und die Zusatznutzen werden zusammenfassend in der folgenden Tabelle überprüft.

[34] Rahmenbedingungen für eine Alleinbezugsverpflichtung sind im „Leitfaden zum Schutz vor Produktpiraterie durch Vertragsgestaltung. Produktpiraterie aus juristischer Sicht: Abwehr von Schutzrechtsverletzungen, Vertragsgestaltung als alternatives Schutzsystem.“ [Gün-11b] dargestellt.

Tabelle 9-4: Abgleich Anforderungen

Nr.			Beschreibung
1			**Anforderungen an Sicherheitsmerkmale**
			siehe Tabelle 7.10
2			**Anforderungen an ein System zur dokumentierten Authentifzierung**
	2.1		**Identifikations- und Prüfpunkte:**
		2.1.1	siehe Tabelle 8.1
		2.1.2	
		2.1.3 ✓	Unmittelbare Mitteilung des Prüfergebnisses an den Prüfer: Neben den in Tabelle 8.1 zusammengefassten Funktionen ist es nun zusätzlich möglich, an den IP-Punkten auf die Prüfergebnisse adäquat zu reagieren (siehe Abschnitt 9.1)
		2.1.4 ✓	Passende systemseitige Reaktion lokal am IP-Punkt: Die verschiedenen Möglichkeiten lokal am IP-Punkt sind im Abschnitt 9.1 dargestellt und zeigen für die verschiedenen Prüfergebnisse adäquate Reaktionen auf. Diese können bei der Implementierung eines Produktpiraterie-Schutzsystems berücksichtigt werden.
		2.1.5	siehe Tabelle 8.1
		2.1.6	
		2.1.7	
		2.1.8	
	2.2		**Gesamtsystem:**
		2.2.1	siehe Tabelle 8.1
		2.2.2	
		2.2.3	
		2.2.4 ✓	Möglichkeit der Integration von systemergänzenden kundenorientierten Dienstleistungen und Zusatzfunktionen zur Generierung einer Win-win-Situation für alle Beteiligten: Die lokal an einem IP-Punkt oder einem Bauteil sowie zentral im System möglichen Zusatznutzen sind in Abschnitt 9.2 beschrieben und können bei der Einrichtung eines Produktpiraterie-Schutzsystems berücksichtigt werden.
		2.2.5	siehe Tabelle 8.1
		2.2.6	
	2.3		siehe Tabelle 8.1
	2.4		**Auswertung:**
		2.4.1 ✓	Zusammenführung, Auswertung und Ausgabe der freigegebenen Daten zu einer Originalware: Neben den in Tabelle 8.1 dargestellten Funktionen ergeben sich aus der Analyse aller Daten aus dem Feld wertvolle Erkenntnisse im Bezug auf die Originalbauteile, die beispielsweise in einer Verschleißprognose dem Kunden wieder zugute kommen (siehe Abschnitt 9.2.2).
		2.4.2	siehe Tabelle 8.1
		2.4.3	Passende systemseitige Reaktionen aus der zentralen Sicht und der Auswertung aller Daten zu einem Bauteil / einer Maschine: Wie die Reaktionen lokal an einem IP-Punkt sind auch die Raktionen aus der zentralen Sicht in Abschnitt 9.1 dargestellt und können bei der Implementierung eines Produktpiraterie-Schutzsystems berücksichtigt werden.

10 Zusammenfassung und Ausblick

10.1 Zusammenfassung

Produkt- und Markenpiraterie ist eine Form der Wirtschaftskriminalität mit erheblichem Ausmaß. Im Jahr 2005 betrug das Geschäft mit kopierten Waren weit mehr als 2% des Welthandelsvolumens (siehe Abschnitt 1.1.3, S. 3). Dies hat Folgen für und Auswirkungen auf die produzierende Industrie, insbesondere die Originalhersteller, aber auch auf die Verbraucher, die weiteren Wirtschaftsbeteiligten und schließlich die gesamte Gesellschaft (siehe Abschnitt 2.3, S. 19).

Um Produkt- und Markenpiraterie entgegen zu wirken gibt es eine Vielzahl an Maßnahmen sowie Vorgehensweisen zur Maßnahmenauswahl. Auch wurde in den letzten Jahren in Deutschland auf Initiative und Förderung des Bundesministeriums für Bildung und Forschung verstärkt im Bereich von „Innovationen gegen Produktpiraterie“ [BMBF-06] in elf parallelen Forschungsprojekten geforscht. Aber, wie aufgezeigt wurde, existiert bisher weder im Maschinen- und Anlagenbau noch in anderen Bereichen ein ganzheitliches technisches Produktpiraterie-Schutzsystem,

- das unterschiedlichste maschinenlesbare, aber auch nicht-maschinenlesbare Sicherheitsmerkmale integrieren kann,
- um Originalkomponenten und -ersatzteile wahlweise als Originale oder als Unikate zu kennzeichnen,
- an IP-Punkten in der Wertschöpfungs- und Logistikkette sowie beim Einsatz in Maschinen und Anlagen zu authentifizieren,
- die Prüfergebnisse im verteilten IT-System gemeinsam mit Tracking&Tracing-Daten zu dokumentieren und
- umfangreiche Systemreaktionen und Zusatznutzen für Kunden, Hersteller und weitere Wirtschaftsbeteiligte zu realisieren.

Diese Funktionen erfüllt das in dieser Arbeit entwickelte Produktpiraterie-Schutzsystem und vereint so den Ansatz des Tracking&Tracing aus der Logistik mit den Möglichkeiten von Sicherheitsmerkmalen in Form von Originalitäts- oder Unikatkennzeichen (siehe hierzu Abschnitt 1.2.2, S. 8).

Um es den Unternehmen im Maschinen- und Anlagenbau zu ermöglichen, dieses technische Produktpiraterie-Schutzsystem zu errichten, wurde in Kapitel 5 als vorbereitender Schritt erarbeitet, wie die Auswahl schützenswerten Bauteile stattfinden kann. Für Bauteile erfolgt in Kapitel 6 die Verwendung von unternehmensspezifischen, rechtlich geschützten Markenzeichen.

Die in Kapitel 7 entwickelten Methoden ermöglichen es, die für ein schützenswertes Bauteil passenden Sicherheitsmerkmale mittels technischer und wirtschaftlicher Kriterien zu bestimmen und an Bauteilen zu applizieren. Damit die technischen Auswahlkriterien auf den Eigenschaften der existierenden Sicherheitsmerkmale angewendet werden können, wurde der aktuell umfangreichste Katalog mit Sicherheitsmerkmalen erarbeitet. Dessen Struktur erlaubt den Unternehmen eine schnelle Orientierung (siehe Anhang A), die tabellarische Darstellung der Eigenschaften der Sicherheitsmerkmale gestattet eine rasche Auswahl der je Bauteil passenden Merkmale (siehe Anhang D). Für die wirtschaftliche Bewertung der technisch passenden Sicherheitsmerkmale wurde ein kombiniertes Vorgehen aus Ansätzen zur monetären Abbildung der Ist-Situation sowie der Kapitalwertmethode und Szenariotechnik für die Bewertung des Plan-Zustands zusammengeführt und detailliert beschrieben. Der abschließende Schritt stellt Eckpunkte der Applikation von Sicherheitsmerkmalen auf den Bauteilen dar.

Es wurde in Kapitel 8 systematisch, strukturiert und detailliert aufgezeigt, wie die ausgewählten Sicherheitsmerkmale optimal in ein technisches Gesamtsystem zur Authentifizierung von Originalbauteilen integriert und zum Schutz der gesamten Wertschöpfungs- und Logistikkette, aber auch der Maschinen und Anlagen bei Kunden eingesetzt werden können. Neben der reinen Überprüfung der Originalität und der Anzeige des Prüfergebnisses an den IP-Punkten wurden in Kapitel 9 auch umfangreiche Zusatznutzen entwickelt, die innerhalb des technischen Gesamtsystems eine Win-win-Situation für alle Wirtschaftsbeteiligten entstehen lassen.

Das gesamte Vorgehen wurde eingebettet in ein schrittweises strategisches Vorgehen. Jeder beschriebene und durchgeführte Einzelschritt wurde an konkreten Beispielen bei ausgewählten Unternehmen validiert. Diese Beispiele sind in der gesamten Arbeit durchgängig vorhanden und wurden schließlich in realen Pilotumsetzungen für den Nachweis der Funktionsfähigkeit des Gesamtsystems zusammengeführt.

Produkt- und Markenpiraterie ist ein sehr komplexes Thema mit verschiedensten technischen, rechtlichen und betriebswirtschaftlichen Aspekten. Die vorliegende Arbeit gibt eine ganzheitliche, logisch aufgebaute, strukturierte Sicht auf das Thema, den hier gewählten Lösungsansatz und die Lösungsentwicklung und füllt die einzelnen Aspekte und Themenfelder inhaltlich vollständig aus. Sie ermöglicht aufgrund der umfassenden Begriffsdefinitionen eine neue sprachliche Koheränz im Themenfeld. Das erarbeitete Produktpiraterie-Schutzsystem schließt die festgestellte Forschungslücke. Die dargestellten Inhalte beschreiben alle wichtigen Themen, die das Produktpiraterie-Schutzsystem betreffen, so dass auch eine praktische Umsetzung in der Industrie direkt möglich ist. Dies ist auch deshalb gewährleistet, da die Funktionsfähigkeit des Gesamtsystems bereits in Demonstratoren sowie Erstumsetzungen in Beispielunternehmen des Maschinen- und Anlagenbaus nachgewiesen werden konnte.

Das entwickelte technische Produktpiraterie-Schutzsystem wirkt aufgrund von sichtbaren Sicherheitsmerkmalen präventiv, kann Kopien eindeutig von Originalbauteilen unterscheiden und ermöglicht somit einen starken und effektiven Produktpirateriesschutz. So sind das gesamte Wertschöpfungs- und Logistiknetzwerk sowie einzelne Maschinen und Anlagen vor dem Eindringen von Kopien, Graumarktware und Waren aus der Dritten Schicht geschützt und es ist ein permanent störungsfreier Betrieb möglich.

10.2 Ausblick

Das in dieser Arbeit entwickelte Produktpiraterie-Schutzsystem kann neben dem Maschinen- und Anlagenbau auch in weiteren Branchen zum Einsatz kommen, beispielsweise der Automobilindustrie. Sicher ist es nicht möglich oder wirtschaftlich sinnvoll, Komponenten und Ersatzteile in den Fahrzeugen selbst mit Hilfe verbauter Identifikations- und Prüfgeräte direkt automatisch zu überprüfen. Aber es könnten die zu verbauenden Teile vor Einbau in ein Fahrzeug auf Originalität geprüft und das Prüfergebnis in die bereits existierenden Digitalen Servicehefte [AUDI-13, Dai-13, Dom-10] eingetragen werden. So wären sowohl Werkstätten als auch Kunden sicher, dass nur Originalbauteile verwendet wurden. Dies garantiert höchste Funktionsfähigkeit und Zuverlässigkeit. Zudem stellt der Nachweis der Verwendung von Originalersatzteilen im eigenen Fahrzeug für Kunden einen geldwerten Nutzen beim Wiederverkauf dar.

Umgekehrt könnte das Digitale Serviceheft der Automobilindustrie wiederum als Vorlage für den Maschinen- und Anlagenbau dienen, um ein je Maschine / Anlage individuelles digitales Serviceheft online zu führen. Das entwickelte Produktpiraterie-Schutzsystem könnte dabei die Daten für dieses digitale Serviceheft liefern. Neben der Anzeige der aktuellen Maschinenstückliste und -konfiguration wäre die Anzeige der Verwendung von Originalteilen ein weiterer Bestandteil dieses Online-Servicehefts.

Die gedankliche Fortführung des Zusatznutzens im Bereich der automatischen Bauteil- und Werkzeugidentifikation“ in Tabelle 9-2 führt zu einer neuen Funktion für Maschinen und Anlagen: „Selbstkonfiguration der Gesamtmaschine bei Verwendung von Originalbauteilen“. Eine solche Funktion hätte in einer Werkzeug-Supply-Chain enormes Kosteneinsparungspotenzial, da das manuelle Einrichten von Maschinen und die händische Eingabe von werkzeugspezifischen Maßen und Betriebsparametern sowohl bei der Werkstückbearbeitung wie auch beim Nachschärfen von Werkzeugen komplett entfallen könnte. Diese Idee wurde seitens des Bundesministeriums für Bildung und Forschung als sehr wertig eingestuft, so dass das durch den Autor beantragte dreijährige Forschungsprojekt „ToolCloud – Unternehmensübergreifendes Lebenszyklusmanagement für Werkzeuge in der Cloud mittels eindeutiger Kennzeichnung und Identifikation“ innerhalb des Zukunftsprojekts Industrie 4.0 ab Oktober 2013 gefördert wird [BMBF-11, fml-13f].

Epilog

Diese Arbeit wurde mit dem Ziel erstellt, Wissen zu schaffen und einen Mehrwert für Wissenschaft und Forschung zu erzeugen. Das Ziel dieser Arbeit ist es aber auch, eine gute Basis für die Entwicklung und Implementierung branchenbezogen passender Produktpiraterie-Schutzsysteme für die Praxis zu schaffen. Der Autor hofft, mit der Ordnung des Themenbereichs mit dem Fokus der Entwicklung eines technischen Produktpiraterie-Schutzsystems für den Maschinen- und Anlagenbau einen neuen Blick auf die Thematik erzeugen zu können und den betroffenen Unternehmen damit die Umsetzung zu erleichtern.

Das Thema Produktpiraterie zu ordnen ist aufgrund seiner Komplexität sehr schwierig, aber notwendig, um neue Lösungen zu finden. „Denken heißt Vergleichen“, so Walther Rathenau, deutscher Politiker und Industrieller[35]. Und die Basis für gute Vergleiche ist Ordnung. Damit ermöglichen Ordnung und Vergleiche einen völlig neuen Blick auf die Dinge selbst (siehe Abbildung 10-1).

Abbildung 10-1: Ordnung und Vergleiche ermöglichen einen völlig neuen Blick auf die Dinge – Werke des Künstlers Ursus Wehrli (Bildquelle: [Hua-11])

[35] * Berlin, 29. September 1867 in, † ebenda, 24. Juni 1922

11 Literaturverzeichnis

[3M-13] 3M: 3M™ Color Floating Image Security Laminate. http://www.3m.com/colorfloatingimage. Letzter Aufruf: 10.01.2013.

[3S-13] 3S Simons Security Systems GmbH: SECUTAG® – Fälschungsschutz für Ihre Originale. http://www.secutag.com/index.php. Letzter Aufruf: 21.01.2013.

[Abe-10] Abele, E.; Albers, A.; Aurich, J.; Günthner, W. (Hrsg.): Wirksamer Schutz gegen Produktpiraterie im Unternehmen – Piraterierisiken erkennen und Schutzmaßnahmen umsetzen. Band 3 der Reihe „Innovationen gegen Produktpiraterie“. VDMA Verlag, Frankfurt am Main: 2010.

[Abe-11] Abele, E.; Kuske, P.; Lang, H.: Schutz vor Produktpiraterie. Ein Handbuch für den Maschinen- und Anlagenbau. Springer, Berlin: 2011.

[Abr-10] Abramovici, M.; Overmeyer, L.; Wirnitzer, B. (Hrsg.): Kennzeichnungstechnologien zum wirksamen Schutz gegen Produktpiraterie. Band 2 der Reihe „Innovationen gegen Produktpiraterie“. VDMA Verlag, Frankfurt am Main: 2010.

[Abr-13] Abramovici, M.: MobilAuthent. www.mobilauthent.de. Letzter Aufruf: 31.01.2013.

[Abs-12] absatzwirtschaft: Service. absatzwirtschaft 6/2003, S. 40. http://www.absatzwirtschaft.de/content/k=UGu6CVw%252beU45VqRl3ToqVxFAZFmJtUZE%252bI8%252bQ7b%252bqVT%252fRpFneJpZixblMypHvIr4dcyvrwX6eyM%253d;showblobms. Letzter Aufruf: 13.11.2012.

[Akt-13] Aktion Plagiarius: Preisträger des Plagiarius. http://www.plagiarius.com/awards.html. Letzter Aufruf: 09.08.2013.

[Ali-13a] Alien Technology Corporation: RFID Tags. http://www.alientechnology.com/tags /index.php. Letzter Aufruf: 17.01.2013.

[Ali-13b] Alien Technology Corporation: Higgs™ 3. EPC Class 1 Gen 2 RFID Tag IC. Alien Technology Corporation, Morgan Hill, USA: 2013.

[Alp-13] AlpVision: Cryptoglyph digital security solution. http://www.alpvision.com/cryptoglyph-covert-marking.html. Letzter Aufruf: 08.01.2013.

[Amt-01] Amtsblatt der Europäischen Union: Richtlinie 2001/83/EG des europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel. ABl. L 311 vom 28.11.2001, S. 67.

[Amt-11] Amtsblatt der Europäischen Union: Richtlinie 2011/62/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Richtlinie 2001/83/EG zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel hinsichtlich der Verhinderung des Eindringens von gefälschten Arzneimitteln in die legale Lieferkette. ABl. L 174/74 vom 01.07.2011, S. 74.

[Amt-12] Amtsblatt der Europäischen Union: Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung). Unterzeichnet in Rom am 25. März 1957. Amtsblatt der Europäischen Union, Brüssel: 2012.

[Arn-08] Arnold, D.; Isermann, H.; Kuhn, A.; Tempelmeier, H.; Furmans, K. (Hrsg.): Handbuch Logistik. 3., neu bearbeitete Auflage. Springer, Berlin und Heidelberg: 2008.

[Arn-10] Arndt, H.: Supply Chain Management. Optimierung logistischer Prozesse.Gabler, Wiesbaden: 2010.

[Art-13] Artikelsicherung.com: Mit amorphen Metallen auf der Jagd nach Ladendieben. http://www.artikelsicherung.com/UserFiles1/Files/AMBeschreibungSiemens.pdf. Letzter Aufruf: 10.01.2013.

[AUDI-13] AUDI AG: Automechanika 2012: Audi Top Service erleben. https://www.audi-mediaservices.com/publish/ms/content/de/public/pressemitteilungen/2012/09/11/automechanika_2012.html. Letzter Aufruf: 19.09.2013.

[Aus-13a] AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H.: Security Features. http://www.austriacard.at/acarticle.jsp#. Letzter Aufruf: 07.01.2013.

[Aus-13b] Austria Card: Together We Can Build a Safer Future. Government. http://www.austriacard.at/download/AC_GOVERNMENT.PDF. Letzter Aufruf: 07.01.2013.

[Ave-13] Avery Dennison Inc.: HF RFID Inlays. AD-709x http://rfid.averydennison.com/products/ad-709x. Letzter Aufruf: 17.01.2013.

[Bad-12] Bader, B.; Helfrich, G.: Explogramme: Mit explosiver Kraft gegen Produktpiraterie. Vortrag zur Tagung: Strategien gegen Produktpiraterie. Lösungen für den Mittelstand, Fraunhofer-Institut für System und Innovationsforschung ISI Karlsruhe, 10. Juli 2012.

[Bae-11] Baetzgen, A. (Hrsg.): Brand planning. Starke Strategien für Marken und Kampagnen. Schäffer-Poeschel, Stuttgart: 2011.

[Ban-05] BankCOLLEG: Firmenkundengeschäft. Schulungsunterlagen. Akademie Deutscher Genossenschaften ADG e.V., Montabaur, 2005. http://gr734heriwzw8262hwhw6262221.genoakademie.de/pages/DozentendownloadFachwirt.268.php?get=494&ei=4WI0Udz0Kcf0sgbr5YHACw&usg=AFQjCNFA2SHf4BKYXHeC4rnLBXCK3tkQEw&bvm=bv.43148975,d.Yms. Letzter Aufruf: 04.03.2013.

[Bar-08] Bartneck, N.; Klaas, V.; Schönherr, H. (Hrsg.): Prozesse optimieren mit RFID und Auto-ID. Grundlagen, Problemlösungen und Anwendungsbeispiele. Publicis Corporate Publishing, Erlangen: 2008.

[Bar-11] Barcodat: 2D-Code-Fibel. Barcodat, Dornstetten: 2011.

[Bar-12] Barker, E.; Barker, W.; Burr, W.; Polk, W.; Smid, M.: Computer Security. Recommendation for Key Management. Part 1: General (Revision 3). NIST – National Institute of Standards and Technology, Gaithersburg: 2012.

[Beh-01] Behrens, M.; Roth, R.: Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven. Friedr. Vieweg, Braunschweig / Wiesbaden: 2001.

[Beh-07] Behrens, B.; Lange, F.; Gastan, E.: Ansatz zur manipulationssicheren Markierung von pulvermetallurgisch hergestellten Bauteilen. http://www.umformtechnik.net/whitepaper/entwicklung-eines -ferti gungsprozessnahen-pruefverfahrens-zur-charakterisierung-der-falzbar keit-von-karosseriefeinblechwerkstoffen_5711. Letzter Aufruf: 19.12.2012.

[Beh-13a] Behr, W.: DNA-Schutz. http://www.dna-schutz.de/kdna-identifizierung. html. Letzter Aufruf: 16.01.2013.

[Beh-13b] Behrens, B.; Lange, F.; Bouguecha, A.; Gastan, E.: Fremdpartikel liefern kodierte Informationen für sicherheitsrelevante Teile. http://www.konstruktionspraxis.vogel.de/themen/werkstoffe /formgebung/articles/113994. Letzter Aufruf: 22.01.2013.

[Ben-10] Bender, J.; Doll, U.; Durchholz, J.; Görtz, M.; Hauck, R.; Kurz, G.; Miller, W.; Pommer, P.; Schlaucher, W.; Stockenberger, D.; Völcker, T.: ProAuthent – Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. Vortrag innerhalb des Industriearbeitskreises des fml - Lehrstuhl für Fördertechnik Materialfluss Logistik der Technischen Universität München, 21. September 2010.

[Ben-12] Bender, J.: Müller Martini GmbH, Zeppelinstrasse 33, 73760 Ostfildern. Expertengespräch am 04.06.2012.

[Ben-13] Bender, J.: Müller Martini GmbH, Zeppelinstrasse 33, 73760 Ostfildern. E-mail des 18.09.2013.

[Ble-13] Bleise, A.: Tailorlux GmbH, Nottulner Landweg 90, 48161 Münster. E-mail des 23.01.2013.

[Blu-06] Blume, A.: Produkt- und Markenpiraterie in der VR China – eine politisch-ökonomische Analyse. Dissertation, Bad Dürkheim: 2006.

[BMBF-06] BMBF – Bundesministerium für Bildung und Forschung: Bekanntmachung. BMBF, Bonn, 08.08.2006. http://www.bmbf.de /foerderungen/6669.php. Letzter Aufruf: 08.11.2012.

[BMBF-11] BMBF – Bundesministerium für Bildung und Forschung: Bekanntmachung. BMBF, Bonn, 19.12.2011 http://www.bmbf.de /foerderungen/17740.php. Letzter Aufruf: 19.09.2013.

[BMBF-12] BMBF – Bundesministerium für Bildung und Forschung : Forschungsoffensive gegen Produktpiraterie. http://www.bmbf.de/de/12095.php. Letzter Aufruf: 14.11.2012.

[BMG-13] BMG – Bundesministerium für Gesundheit: Arzneimittelfälschungen - ein globales Problem. http://www.bmg.bund.de/krankenversicherung/arzneimittelversorgung/arzneimittelfaelschungen.html. Letzter Aufruf: 01.03.2013.

[BMI-13] BMI – Bundesministerium des Inneren: Warum wurden Gesicht und Fingerabdruck als biometrische Merkmale für den ePass ausgewählt? http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen /Sicherheit/biometrie_faq_ausgewaehlt.html. Letzter Aufruf: 18.02.2013.

[BMJ-13a] BMJ – Bundesministerium der Justiz: Gesetz gegen Wettbewerbsbeschränkungen. http://www.gesetze-im-internet.de/gwb. Letzter Aufruf: 29.05.2013.

[BMJ-13b] BMJ – Bundesministerium der Justiz: Gesetz gegen den unlauteren Wettbewerb. http://www.gesetze-im-internet.de/uwg_2004. Letzter Aufruf: 29.05.2013.

[BMJ-13c] BMJ – Bundesministerium der Justiz: Gesetz über die Haftung für fehlerhafte Produkte. http://www.gesetze-im-internet.de/prodhaftg /index.html. Letzter Aufruf: 15.09.2013.

[BMJ-13d] BMJ – Bundesministerium der Justiz: Bürgerliches Gesetzbuch. http://www.gesetze-im-internet.de/bgb. Letzter Aufruf: 15.09.2013.

[BMJ-13e] BMJ – Bundesministerium der Justiz: Gesetz über den Schutz von Marken und sonstigen Kennzeichen.http://www.gesetze-im-internet.de/markeng. Letzter Aufruf: 22.09.2013.

[BMWi-11] BMWi – Bundesministerium für Wirtschaft und Technologie (Hrsg.): Schlaglichter der Wirtschaftspolitik. Monatsbericht August 2011.

Bundesministerium für Wirtschaft und Technologie (BMWi), Berlin: 2011.

[Boc-13] Bockhorni, F.; Schuberth, S.: Genetischer Fingerabdruck für Medikamente. DNA-Labeling sorgt für Fälschungssicherheit. http://www.labo.de/bio-cluster-und-applikationen/Bio-Cluster-und-Applikationen---DNA-Labeling.htm. Letzter Aufruf: 09.01.2013.

[Böh-06] Böhmann, T.; Krcmar, H.: Komplexitätsmanagement als Herausforderung hybrider Wertschöpfung im Netzwerk. In: Wojda, F.; Barth, A.: Innovative Kooperationsnetzwerke. Deutscher Universitäts-Verlag, Wiesbaden: 2006, S. 81-106.

[Bra-99] Braatz, F.; Brinker, U.: Friedrich, H.-J. (Hrsg.): Alles über Zahlungsverkehr mit Karten. Kreditkarten, Scheckkarten, Kundenkarten, Geldkarten, Anbieter, Marktdaten, Technik, Sicherheit. Luchterhand, Neuwied und Kriftel: 1999.

[Bra-08a] Brand, S.: VOLLMER WERKE Maschinenfabrik GmbH, Ehinger Straße 34, 88400 Biberach / Riß. Gespräch am 07.05.2008.

[Bra-08b] Braun, M.: Fälschungssichere RFID-Chips. Siemens AG, 2008. http://mobkom.files.wordpress.com/2008/05/5-dr-braun-falschungssichere-rfid-chips.pdf. Letzter Aufruf: 12.08.2013.

[Bre-02] Bretzke, W.; Stölzle, W.; Karrer, M.; Ploenes, P.: Vom Tracking & Tracing zum Supply Chain Event Management – aktueller Stand und Trends. KPMG Consulting GmbH, Berlin: 2002.

[Bro-12a] Brockhaus Enzyklopädie Online: Fälschung. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12b] Brockhaus Enzyklopädie Online: Imitat. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12c] Brockhaus Enzyklopädie Online: Konfuzius. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12d] Brockhaus Enzyklopädie Online: Lizenzprodukt. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12e] Brockhaus Enzyklopädie Online: Nachahmung. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12f] Brockhaus Enzyklopädie Online: Original. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12g] Brockhaus Enzyklopädie Online: Plagiat. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-12h] Brockhaus Enzyklopädie Online: Replik. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 31.10.2012.

[Bro-13a] Brockhaus Enzyklopädie Online: Fluoreszenz. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 23.01.2013.

[Bro-13b] Brockhaus Enzyklopädie Online: Phosphoreszenz. http://www.brockhaus-enzyklopaedie.de/be21_article.php. Letzter Aufruf: 23.01.2013.

[Bro-13c] Brockhaus Enzyklopädie Online: Szenariotechnik. https://emedia1.bsb-muenchen.de/han/BROCKHAUSWISSENSSERVICE/https/bsb.brockhaus-wissensservice.com/brockhaus/ szenario-technik. Letzter Aufruf: 07.07.2013.

[Bro-13d] Brockhaus Enzyklopädie Online: Produktlebenszyklus. http://emedia1.bsb-muenchen.de/han/BROCKHAUSWISSENSSERVICE/https/bsb.brockhaus-wissensservice.com/brockhaus/produktlebenszyklus. Letzter Aufruf: 14.07.2013.

[Bro-13e] Brockhaus Enzyklopädie Online: Emulation. http://emedia1.bsb-muenchen.de/han/BROCKHAUSWISSENSSERVICE/https/bsb.brockhaus-wissensservice.com/brockhaus/emulation-informatik. Letzter Aufruf: 12.08.2013.

[Brü-09] Brüll, L.: Protexxion – eine neue Technologie der Bayer Technology Services zum Schutz vor Fälschungen. Vortrag beim Presse-

Workshop der LOG mbH: Supply Chain und Produktpiraterie – Innovation im Bereich fälschungssichere Kennzeichnung und mobile Authentifizierung von Produkten, Bonn, 05. - 06.11.2009.

[Bru-13] Brunthaler, S.: Tracking & Tracing. Verfolgung von beweglichen Objekten im Transport- und Verkehrsgeschehen mit Hilfe der IT. http://www.tfh-wildau.de/sbruntha/Material/LTM/Verkehrslogistik/VL_LTM_TL_TrackingTracing.pdf. Letzter Aufruf: 08.08.2013.

[BSI-13a] BSI – Bundesamt für Sicherheit in der Informationstechnik: Grundsätzliche Funktionsweise biometrischer Verfahren. https://www.bsi.bund.de/ContentBSI/Themen/Biometrie/AllgemeineEinfuehrung/einfuehrung.html;jsessionid=CCC5F773F10726C9446605C0EDD584A8 .2_cid294. Letzer Aufruf: 18.02.2013.

[BSI-13b] BSI – Bundesamt für Sicherheit in der Informationstechnik: Sicherheitsgateway (Firewall). https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Content_Cyber-Sicherheit/ThemenCS/Sicherheitskomponenten/Sicherheitsgateway/loesungen_firewall.html. Letzter Aufruf: 24.08.2013.

[BSI-13c] BSI – Bundesamt für Sicherheit in der Informationstechnik: B 3.301 Sicherheitsgateway (Firewall). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03301.html. Letzter Aufruf: 24.08.2013.

[BSI-13d] BSI – Bundesamt für Sicherheit in der Informationstechnik: B 5.7 Datenbanken. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05007.html. Letzter Aufruf: 05.09.2013.

[Bun-05] Bundesdruckerei: Pocket Guide to ePassport Systems. Bundesdruckerei GmbH, Berlin: 2005.

[Bun-09] Bundesgesetzblatt: Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften vom 18. Juni 2009. Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 33, ausgegeben zu Bonn am 24. Juni 2009.

[Bun-12a] Bundesdruckerei: eID-KARTE. Pocket guide 2012. Bundesdruckerei GmbH, Berlin: 2012.

[Bun-87] Bundesgesetzblatt: Gesetz über den Schutz der Topographien von mikroelektronischen Halbleitererzeugnissen (Halbleiterschutzgesetz) vom 22. Oktober 1987. Bundesgesetzblatt, Jahrgang 1987, Teil I, Bonn, den 22 Oktober 1987, S. 2294 ff.

[Bun-97] Bundesgesetzblatt: Bekanntmachung der Neufassung des Sortenschutzgesetzes vom 19. Dezember 1997. Bundesgesetzblatt Jahrgang 1997 Teil I Nr.87, ausgegeben zu Bonn am 29. Dezember 1997, S. 3164 ff.

[Bun-12b] Bundesgesetzblatt: Zweites Gesetz zur Änderung arzneimittelrechtlicher und anderer Vorschriften vom 19. Oktober 2012. Bundesgesetzblatt Jahrgang 2012 Teil I Nr. 50, ausgegeben zu Bonn am 25. Oktober 2012.

[Bun-13a] Bundesdruckerei: Zukunft sichern. Die Forschungsarbeit der Bundesdruckerei. http://www.bundesdruckerei.de/de/226-innovationen-schaf fen. Letzter Aufruf: 09.01.2013.

[Bun-13b] Bundesdruckerei: Ausweis. Identitätsdokument für die reale und die digitale Welt. http://www.bundesdruckerei.de/de/94-neuer-personal ausweis. Letzter Aufruf: 30.01.2013.

[Bun-13c] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. Übersicht über geeignete Algorithmen. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mainz: 2013.

[cab-13] cab Etikettiersysteme: Barcode-Lexikon. http://www.haug-remchingen.de/cab_eti_1/Barcodes/code-lexi.html. Letzter Aufruf: 19.07.2013.

[Cat-05] Cattaui, M. L.: Counterfeiting is out of control. 13.05.2005. http://www.iccwbo.org/News/Articles/2005/Counterfeiting-is-out-of-control. Letzter Aufruf: 09.08.2013.

[Cha-05] Chaffey, D.; Wood, S.: Business Information Management. : Improving Performance Using Information Systems. FT Prentice Hall, Harlow: 2005.

[Chi-04] Chip Online: Nokia bietet Internet-Prüfung für Handy-Akkus. http://www.chip.de/news/Nokia-bietet-Internet-Pruefung-fuer-Handy-Akkus_12801306.html. CHIP Xonio Online GmbH, München, 2004. Letzter Aufruf: 21.06.2013.

[Con-13] Consolidated Printing, Inc.: Security Features. http://www.teamcpi.com /security-coin.html. Letzter Aufruf: 21.01.2013.

[Cor-13] Corduwinus, D.; Wander, S.; Wensing, T.; Wyen, D.: Save your Brand. Brand Protection durch die Druck- und Medienindustrie. http://saveyourbrand.de/%5BSAVE%20YOUR%20BRAND%5D_die_Brosch%C3%BCre.pdf. Letzter Aufruf: 10.01.2013.

[Dai-13] Daimler AG: Der Mercedes-Benz Digitaler Servicebericht. http://www.mercedes-benz.de/content/germany/mpc/mpc _germany_website/de/home_mpc/passengercars/home/servicesandaccessories/services_online/digital_servicereport.html. Letzter Aufruf: 19.09.2013.

[Dat-07] Datalogic: Strichcode-Fibel. Datalogic, Lippo di Calderara di Reno Bologna: 2007.

[Dat-13a] DataDot Technology USA Inc: DataTraceDNA®. http://www.datadotdna.com/us/brand_datatrace.php. Letzter Aufruf: 09.01.2013.

[Dat-13b] DataDot Technology Ltd: AuthentiCable™. http://www.datadotdna.com/brand_authenticable.php. Letzter Aufruf: 17.01.2013.

[Dat-13c] DataTraceDNA Pty Ltd.: DataTraceDNA - Moleküler Ürün Kodlama ve Takip Teknolojisi. http://www.datatracedna.com.tr. Letzter Aufruf: 17.01.2013.

[Dat-13d] DataDot Malaysia Sdn Bhd: DataLabel DNA. http://datadot.com.my/blog/products/datalabel-dna. Letzter Aufruf: 21.01.2013.

[DB-12] DB Fernverkehr AG: Beförderungsbedingungen der Deutschen Bahn AG. DB Fernverkehr AG, Frankfurt am Main: 2012.

[Dei-13] Deichmann, E.: Deutsche Bahn Vertrieb GmbH, Frankenallee 2-4, 60327 Frankfurt am Main. E-mail und Präsentation des 20.03.2013.

[Den-08] Denkler, T.: Das Verbrechen des 21. Jahrhunderts. 16.12.2008. http://www.sueddeutsche.de/wirtschaft/produktpiraterie-das-verbrechen-des-jahrhunderts-1.787790. Letzter Aufruf: 09.08.2013.

[Deu-13a] Deutsche Bundesbank: Falschgelderkennung. http://www.bundesbank.de/Navigation/DE/Kerngeschaeftsfelder/Bargeld/Falschgeld/Falschgelderkennung/falschgelderkennung.html. Letzter Aufruf: 18.01.2013.

[Deu-13b] Deutsche Physikalische Gesellschaft e.V.: Was verrät die Röntgenfluoreszenzanalyse? http://www.weltderphysik.de/gebiete/atome/syn chrotronstrahlung/roentgenfluoreszenzanalyse/roentgen fluoreszenzanalyse. Letzter Aufruf: 18.01.2013.

[Deu-13c] Deutsche Post DHL: DHL Active Tracing. Viel mehr als Track & Trace. http://www.dhl.de/content/dam/dhlde/logistik/pdf/freight-05-2011/dhl -logistik-active-tracing-05-2011.pdf. Letzter Aufruf: 14.05.2013.

[Deu-13d] Deutsche Post AG: DHL Paketmarke Deutschland bis 10 kg. einzeln. https://www.efiliale.de/efiliale/katalog/produktDHL.jsp?Item=prod6220042&parentCat=cat48040108. Letzter Aufruf: 22.07.2013.

[Dia-13] Diagramm Halbach GmbH & Co. KG: Fahrscheine. http://www.halbach.com. Letzter Aufruf: 18.01.2013.

[Die-08] Dierig, C.: Deutsche fälschen ihre Maschinen gerne selbst. In: Die Welt, 22.04.2008. http://www.welt.de/wirtschaft/article1928254/Deutsche-faelschen-ihre-Maschinen-gerne-selbst.html. Letzter Aufruf: 09.08.2013.

[DIN16557-5] DIN 16557-5:2002. Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT). Teil 5: Regeln zur Generierung

von XML-Schema-Dateien (XSD) aus EDI(FACT)-Anwendungsbeschreibungen. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735] DIN ISO 9735:2002: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-1] DIN ISO 9735-1:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 1: Syntax-Regeln, die für alle Teile gemeinsam sind. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-10] DIN ISO 9735-10: 2004. Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 10: Syntax-Service-Verzeichnisse. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-2] DIN ISO 9735-2:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 2: Syntax-Regeln für Batch-EDI. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-3] DIN ISO 9735-3:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 3: Syntax-Regeln für Interaktiv-EDI. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-4] DIN ISO 9735-4:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 4: Syntax- und Servicebericht für Batch-EDI (Nachrichtentyp - CONTRL). Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-5] DIN ISO 9735-5:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 5: Sicherheitsregeln für Batch-EDI (Authentizität, Integrität und Unbestreitbarkeit des Ursprungs). Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-6] DIN ISO 9735-6: 2004. Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 6: Sicherheits-Authentisierung und -Bestätigung. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-7] DIN ISO 9735-7:2004. Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene. Teil 7: Sicherheitsregeln für Batch-EDI (Vertraulichkeit). Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-8] DIN ISO 9735-8:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) - Syntax-Regeln auf Anwendungsebene. Teil 8: Eingebundene Daten in EDI. Deutsches Institut für Normung e.V. Berlin: Beuth.

[DIN9735-9] DIN ISO 9735-9:2004: Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene Teil 9: Sicherheitsschlüssel- und Zertifikats-Verwaltung (Nachrichtentyp - KEYMAN). Deutsches Institut für Normung e.V. Berlin: Beuth.

[Dir-10] Direction générale de la compétitivité de l'industrie et des services: Guide pratique pour mettre en oevre les solutions d'authentification des produits manufactures. DGCIS, Paris: 2010.

[Dol-08] Doll, U.: HOMAG Holzbearbeitungssysteme GmbH, Homagstrasse 3-5, 72296 Schopfloch. Expertengespräch am 08.05.2008.

[Dol-10] Doll, U.: Forum "Produktpiraten und Raubkopierer - Die Konkurrenz um pfiffige Logistiklösungen ist gross, der Ideenklau gang und gäbe". Vortrag auf der LogiMAT 2012, 10. Internationale Fachmesse für Distribution, Material- und Informationsfluss. Landesmesse am Stuttgarter Flughafen, 13. – 15.03.2012.

[Dol-13] Doll, U.: HOMAG Holzbearbeitungssysteme GmbH, Homagstrasse 3-5, 72296 Schopfloch. Expertengespräch am 01.08.2013.

[Dom-05] Domizlaff, H.: Die Gewinnung des öffentlichen Vertrauens: ein Lehrbuch der Markentechnik. Marketing-Journal, Hamburg: 2005.

[Dom-10] Dominsky, S.: Servicehefte: Wettbewerbsknebel oder digitaler Fortschritt? Jeder kocht sein eigenes Süppchen. In: Kfz-Betrieb, Vogel Medien, Würzburg: 2010. http://www.kfz-betrieb.vogel.de /service/praxis/articles/264408. Letzter Aufruf: 19.10.2013.

[DPMA-08] DPMA – Deutsches Patent- und Markenamt (Hrsg.): Patente. Eine Informationsbroschüre zum Patent. Deutsches Patent- und Markenamt, München: 2008.

[DPMA-12] DPMA – Deutsches Patent- und Markenamt: Patentschutz. http://www.dpma.de/patent/patentschutz/index.html. Letzer Aufruf: 07.11.2012.

[DPMA-13] DPMA – Deutsches Patent- und Markenamt: Patente. http://presse.dpma.de/presseservice/datenzahlenfakten/statistiken /patente/index.html. Letzter Aufruf: 31.05.2013.

[Dri-07] Drives&Controls: Fake engineering products are costing ‘thousands’ of jobs. 11.04.2007. http://drivesncontrols.com/news /archivestory.php/aid/1435/Fake_engineering_products_are_ costing__91thousands_92_of_jobs.html. Letzter Aufruf: 09.08.2013.

[Dru-13] Drucktechniken.de: Siebdruck. http://www.drucktechniken.de/sieb druck_englisch.html. Letzter Aufruf: 17.01.2013.

[Dun-08] Dunkel, J.; Eberhart, A.; Fischer, S.; Kleiner, C.; Koschel, A.: Systemarchitekturen für verteilte Anwendungen. Carl Hanser, München: 2008.

[Dur-12] Durchholz, J.; Stockenberger, D.; Günthner, W.: Präventiver Produktpirateriesschutz. Einsatz von passiven, signierten RFID-Transpondern im Maschinen- und Anlagenbau. In: Industrie Management. Zeitschrift für industrielle Geschäftsprozesse. 28. Jahrgang (2012) Nr. 4. S. 11-14.

[Eck-08] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg, München: 2008.

[Eco-13] ECOIN Vertriebs & Service Ltd.: Banknoten-Prüfgerät UV 20 http://www.ecoin-systeme.de/muenz-und-banknoten-pruefgeraete/banknoten-pruefgeraet-uv-20.html. Letzter Aufruf: 14.02.2013.

[Ein-12] EINS GmbH – Entwicklung Interaktiver Software: O-PUR. www.opur-secure.com. Letzter Aufruf: 08.11.2012.

[Ele-13] Electronic Frontier Foundation: Investigating Machine Identification Code Technology in Color Laser Printers. https://w2.eff.org/Privacy/printers/wp.php. Letzter Aufruf: 18.01.2013.

[EPC-07] EPCglobal: EPC Information Services (EPCIS) Version 1.0.1 Specification. EPCglobal, Brüssel, 2008.

[EPC-08] EPCGlobal Inc.: EPC™ Radio-Frequency Identity Protocols. Class-1 Generation-2 UHF RFID. Protocol for Communications at 860 - 960 MHz. Version 1.2.0. GS1 EPCglobal, Brüssel, 2008.

[EPC-10] EPCGlobal Inc.: Core Business Vocabulary Standard. EPCglobal, Brüssel, 2008.

[EPO-13] EPO - Europäische Patentorganisation: Europäische Patentanmeldungen insgesamt. http://www.epo.org/about-us/annual-reports-statistics/statistics/filings_de.html. Letzter Aufruf: 31.05.2013.

[Esc-05] Esch, F.: Moderne Markenführung: Grundlagen, innovative Ansätze, praktische Umsetzungen. Gabler, Wiesbaden: 2005.

[Esc-12] Esch, F.: Strategie und Technik der Markenführung. Vahlen, München: 2012.

[EZB-13a] EZB – Europäische Zentralbank: Forschung und Entwicklung im Bereich Banknoten – Möglichkeiten zur Zusammenarbeit mit der EZB. http://www.ecb.int/euro/html/research.de.html. Letzter Aufruf: 09.01.2013.

[EZB-13b] EZB – Europäischen Zentralbank: Die Sicherheitsmerkmale der Euro-Banknoten. http://www.ecb.int/euro/html/security_features.de.html. Letzter Aufruf: 14.02.2013.

[Fac-13] Fachhochschule Köln, Campus Gummersbach: Datenbanken Online Lexikon. http://wikis.gm.fh-koeln.de/wiki_db/Onlinelexikon /Startseite. Letzter Aufruf: 05.09.2013.

[Fae-07] Faeskorn-Woyke, H.; Bertelsmeier, B.; Riemer, P.; Bauer, E.: Datenbanksysteme. Theorie und Praxis mit SQL2003, Oracle und MySQL. Pearson Studium, München: 2007.

[Fah-10] Fahry, G.: Fälschungssichere Fingerabdrücke. In: FM. Das Logistik-Magazin. 42. Jahrgang (2010) Nr. 12 S. 38-39.

[Fer-92] Ferraiolo, D.; Kuhn, R: Role-Based Access Controls. In: National Institute of Standards and Technology, Proceedings 15th National Computer Security Conference 1992, National Computer Security Center, Baltimore Convention Center, Baltimore, 13. - 16. Oktober 1992. S. 554 - 563.

[Fin-12] Finkenzeller, K.: RFID-Handbuch. Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC. Carl Hanser, München: 2012.

[Fle-05] Fleisch, E.; Mattern, F. (Hrsg.): Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis. Springer, Berlin: 2005.

[fml-13a] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. www.proauthent.de. Letzter Aufruf: 24.05.2013.

[fml-13b] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: ProAuthent - Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. http://www.fml.mw.tum.de/fml/index.php?Set_ID=270. Letzter Aufruf: 24.05.2013.

[fml-13c] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: Logistikkompendium. RFID. http://www.fml.mw.tum.de/fml/index.php? Set_ID =945&letter=R&title=RFID. Letzter Aufruf: 24.07.2013.

[fml-13d] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: Logistikkompendium. RFID-Transponder. http://www.fml.mw.tum.de /fml/index.php?Set_ID=945&letter=R&title=RFID-Transponder. Letzter Aufruf: 27.07.2013.

[fml-13e] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: Logistikkompendium. Supply Chain Management. http://www.fml.mw.tum .de/fml/index.php?Set_ID=945&letter=S&title=Supply_Chain_Management. Letzter Aufruf: 19.08.2013.

[fml-13f] fml – Lehrstuhl für Fördertechnik Materialfluss Logistik: ToolCloud - Unternehmensübergreifendes Lebenszyklusmanagement für Werkzeuge in der Cloud mittels eindeutiger Kennzeichnung und Identifikation. http://www.fml.mw.tum.de/fml/index.php?Set_ID=1002. Letzter Aufruf: 02.12.2013.

[Fon-13] FontShop AG: Die 100 besten Schriften aller Zeiten. http://www .100besteschriften.de/index.php. Letzter Aufruf: 19.07.2013.

[Fra-11] Fraunhofer-Institut für Chemische Technologie ICT: Sprengprägen zur Strukturierung von Werkzeugen und Metalloberflächen. Fraunhofer-Institut für Chemische Technologie ICT, Pfinztal (Berghausen): 2011.

[Fra-12] Fraunhofer-Gesellschaft: Maschine mit Kopierschutz. In: weiter.vorn 4.2012. http://www.fraunhofer.de/de/publikationen /fraunhofer-magazin /2012/weitervorn_4-2012_Inhalt/weitervorn_4-2012_42.html. Letzter Aufruf: 22.10.2012.

[Fuc-06] Fuchs, H. (Hrsg.); Kammerer, J.; Ma, X.; Rehn, I.: Piraten Fälscher und Kopierer. Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China. Gabler, Wiesbaden: 2006.

[Fuc-09] Fuchs, H.; Zhou, S.: Lohnt sich die Bekämpfung der Produkt- und Markenpiraterie? In: IP-Manager. AV-News GmbH, München: 3/2009. Download möglich unter http://www.chinabrand.de /publikationen /download-document/68-lohnt-sich-die-bekampfung-der-produkt-und-markenpiraterie-german.html. Letzter Aufruf: 05.07.2013.

[Fuc-12] Fuchs, H.: CHINABRAND CONSULTING LTD., Am Blütenanger 55, 80995 München. Gespräch am 16.11.2012.

[Fuc-13] Fuchs, H.: CHINABRAND CONSULTING LTD., Am Blütenanger 55, 80995 München. E-Mail des 10.07.2013.

[Gat-13] Gate4Logistics.de: Top-Ten Logistik-Unternehmen. Top 10 weltweit. http://www.gate4logistics.de/logistik-karriere/top-10-unternehmen .html. Letzter Aufruf: 14.05.2013.

[Gau-10] Gausemeier, J. (Hrsg.): Innovationen gegen Produktpiraterie. Produktschutz kompakt. Heinz Nixdorf Institut, Paderborn: 2010.

[Gau-12] Gausemeier, J.; Glatz, R.; Lindemann, U.: Präventiver Produktschutz. Leitfaden und Anwendungsbeispiele.

[GdP-10] GdP – Gewerkschaft der Polizei: Definitionen. In: Produkt- und Markenpiraterie. Verlag Deutsche Polizeiliteratur, Hilden: 2010.

[Ger-07] Gerber, T.; Labusga, S.: Abgewogen. Ersatztinte für Brother, Canon, HP und Lexmark. In: c't magazin für computer technik (2007) Nr. 17, S. 132-144.

[Ger-08] Zurückgesetzt. In: c't magazin für computer technik (2008) Nr. 14, S. 62.

[Ger-09] Gerber, T.; Labusga, S.: Alternativ. Günstige Tinte für Drucker und Multifunktionsgeräte von Brother, Canon, Epson und Hewlett-Packard. In: c't magazin für computer technik (2009) Nr. 12, S. 104-111.

[Gie-13a] Giesecke & Devrient GmbH: Glossar der Fachausdrücke. http://www.gi-e.com/de/about_g_d/services/glossary/glossary.jsp. Letzter Aufruf: 08.01.2013.

[Gie-13b] Giesecke & Devrient GmbH: Fenster in Banknoten. http://www.gi-de.com/de/products_and_solutions/products/security_features/Windows-in-banknotes-3394.jsp. Letzter Aufruf: 17.01.2013.

[Gie-13c] Giesecke & Devrient GmbH: Prinzregentenstraße 159, 81677 München. Mündliche Auskunft am 17.02.2013.

[Gla-03] Glauner, C.; Korte, S.: Forschungsbericht. Ingenieur-Dienstleistungen. Zukünftige Technologien Consulting des VDI-Technologiezentrums, Düsseldorf: 2003.

[Glo-06] Glover, B.; Bhatt, H.: RFID Essentials. O'Reilly Media, Sebastopol (USA): 2006.

[Goo-13a] Google.de: Produktpiraterie. www.google.de. Letzter Aufruf: 29.01.2013.

[Goo-13b] Google.de: Counterfeiting. www.google.de Letzter Aufruf: 29.01.2013.

[Gra-13] Graßmann, A.: Patentanmeldungen. http://www.patent-page.de/patentanmeldungen. Letzter Aufruf: 31.05.2013.

[Gri-08] Griffiths-Harvey, M.; Neill, B.; Smith, K.; Rosati, T.; Davis, W.; Walters, A.; Tsang, R.; Brown, D.; Vanstone, S.; Certicom Corp., Kanada: Authenticated Radio Frequency Identification and Key Distribution System therefor. Patentschrift WO 2008/028291 A1, 13. März 2008.

[GS1-13a] GS1 – Global Standards One. http://www.gs1.org. Letzter Aufruf: 21.08.2013.

[GS1-13b] GS1 AISBL: EPC Tag Data Standard 1.7. GS1 AISBL, Brüssel: 2013.

[GS1-13c] GS1: GS1 General Specifications. Version 13.1. GS1, Brüssel: 2013.

[GS1-13d] GS1: The GS1 EPCglobal Architecture Framework. GS1, Brüssel: 2013.

[GS1-13e] GS1: Discovery Services Standard (in development). http://www.gs1.org/gsmp/kc/epcglobal/discovery. Letzter Aufruf: 10.09.2013.

[Gud-12] Gudehus, T.: Logistik 1. Grundlagen, Verfahren und Strategien. Springer, Berlin, Heidelberg: 2012.

[Gün-06a] Günthner, W. A.; Kessler, S.; Sanladerer, S.: Transportlogistik am Bau. Entwicklung eines Planungs- und Kontrollinstruments mit integrierter Datenerfassung und -bewertung für den Transport veredelter Schütt- und Stückgüter in der Bauindustrie. fml – Lehrstuhl für Fördertechnik Materialfluss Logistik, Garching: 2006.

[Gün-06b] Günthner, W. A.: Schutz der Supply Chain mit Originalitäts- und Unikatkennzeichnungen. Durchgehende Produktverfolgung mit Tracking & Tracing. Vortrag zur Tagung: Produktpirateriesschutz im Unternehmen. Sicherung von Absatz und Know-how. TCW Transfer-Centrum GmbH & Co. KG, München, 20. - 21. Juni 2007.

[Gün-08] Günthner, W. A.; Durchholz, J.; Meißner, S.; Stockenberger, D.: Potenziale des Produktpirateriesschutzes durch kognitive Authentifizierung. In: Industrie Management. Zeitschrift für industrielle Geschäftsprozesse. 24. Jahrgang (2008) Nr. 6. S. 23-27.

[Gün-10] Günthner, W. A.; ten Hompel, M. (Hrsg.): Internet der Dinge in der Intralogistik. Springer, Heidelberg: 2010.

[Gün-11a] Günthner, W. A. (Hrsg.); Durchholz, J.; Stockenberger, D., Wildemann, H.; Pommer, P.; Tschöke, T; Völcker, T.: Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung. Bestimmung schützenswerter Bauteile, Auswahl von Kennzeichnungstechnologien und Gestaltung des Schutzsystems. Lehrstuhl für Fördertechnik Materialfluss Logistik (fml), München: 2011.

[Gün-11b] Günthner, W. A. (Hrsg.); Ann, C.; Hauck, R.; Durchholz, J.; Stockenberger, D.: Leitfaden zum Schutz vor Produktpiraterie durch Vertragsgestaltung. Produktpiraterie aus juristischer Sicht: Abwehr von Schutzrechtsverletzungen, Vertragsgestaltung als alternatives Schutzsystem. Lehrstuhl für Fördertechnik Materialfluss Logistik (fml), München: 2011.

[Gün-11c] Günthner, W. A.; Durchholz, J.; Stockenberger, D.: Schlussbericht für das Forschungsprojekt ProAuthent. Integrierter Produktpirate-

rieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. fml - Lehrstuhl für Fördertechnik Materialfluss Logistik, Technische Universität München, München, 2011.

[Gün-11d] Günthner, W. A.; Köster, O.; Oldendorf, C.: Technische Schutzmaßnahmen gegen Produktpiraterie. In: Freimuth, J.; Krieg, R.; Luo, M.; Müller, C.; Schädler, M. (Hrsg.): Geistiges Eigentum in China. Neuere Entwicklungen und praktische Ansätze für den Schutz und Austausch von Wissen. Galber/Springer, Wiesbaden: 2011.

[Gün-12a] Günthner, W. A.; Prives, S.; Biebl, E.; Loibl, C.: Intelligente Thermobehälter. In: Logistik Heute. Das deutsche Logistikmagazin. 34. Jahrgang (2012) Nr. 12. S. 28 f.

[Gün-12b] Günthner, W. A.: Materialfluss und Logistik. Vorlesungsskriptum: Lehrstuhl für Fördertechnik Materialfluss Logistik. Technische Universität München: 2012.

[Gün-13a] Günthner, W. A.: Planung technischer Logistiksysteme. Vorlesungsskriptum: Lehrstuhl für Fördertechnik Materialfluss Logistik. Technische Universität München: 2013.

[Gün-13b] Günthner, W. A.; Durchholz, J.; Klenk, E.; Boppert, J.: Schlanke Logistikprozesse. Handbuch für den Planer. Springer, Berlin: 2013.

[Ham-13] Hammerschmidt, C.: Maschinenbauer rüsten auf gegen Produktpiraten. http://www.vdi-nachrichten.com/artikel/Maschinenbauer-ruesten-auf-gegen-Produktpiraten/58566/2. Letzter Aufruf: 17.01.2013.

[Hei-12] Heinz Nixdorf Institut, Universität Paderborn: ConImit. www.conimit.de. Letzter Aufruf: 08.11.2012.

[Hei-13] Heimann-Heinevetter, A.: Der abhängige Mensch. http://www.pflege-kurse.de/006kursdemo01.asp?KID=7 &seitennummer=4. Letzter Aufruf: 17.01.2013.

[Her-11] Herwig, M.: Produktpiraterie kostet Millionen. Die Industrie führt einen mühsamen Kampf gegen die Produktfälscher. In: Badische Neueste Nachrichten (2011) Nr. 266, S. 9.

[Hoc-13] Hochschule für Technik, Wirtschaft und Kultur Leipzig: Veredelungslexikon. Prägen. http://www.veredelungslexikon.htwk-leipzig.de/de/ver edeln-durch-umformen/praegen. Letzter Aufruf: 09.01.2013.

[Hof-10] Hoffmann, K.: Produktpiraterie in der Investitionsgüterindustrie - Situationsanalyse und Abwehrstrategien. GRIN Verlag, München: 2010.

[Hom-06] ten Hompel, M.; Heidenblut, V.: Taschenlexikon Logistik. Abkürzungen, Definitionen und Erläuterungen der wichtigsten Begriffe aus Materialfluss und Logistik. Springer, Berlin und Heidelberg: 2006.

[Hom-12] Homag Holzbearbeitungssysteme AG: ProAuthent. www.proauthent. de. Letzter Aufruf: 08.11.2012.

[Hop-03] Hopkins, D.; Kontnik, L.; Turnage, M.: Counterfeiting Exposed. Protecting Your Brand and Customers. Wiley & Sons, New Jersey: 2003.

[Hot-11] Hottmann, S.; Fiedler, D.: Forschungsbericht IW 090065. Neuartiger Produktschutz durch Antigen-Antikörper Reaktionen mittels Nano-sol- Immobilisierung auf Papier. PTS - Papiertechnische Stiftung, Heidenau, München: 2011.

[Hua-11] Huang, J.: The Art of Clean Up: Sorting and Stacking Everyday Objects. Jeannie, Jeannie Jeannie – Design Finds fort he Creative Minds: 29.08.2011. http://www.jeanniejeannie.com/2011/08/the-art-of-clean-up-sorting-and-stacking-everyday-objects. Letzter Aufruf: 19.09.2013.

[Hub-10] Huber, A.: Informationsschutz im Mittelstand. Wie sicher sind Ihre Geschäftsgeheimnisse? In: VBKI Spiegel, 60. Jahrgang (2010), Nr. 218, S. 22 - 23.

[Hun-06] Hundsdörfer, R.: Produktpiraterie. Alles nur geklaut. In: MaschinenMarkt. Das Industrieportal. 30.05.2006. http://www.maschinenmarkt.vogel.de/index.cfm?pid=1850&pk=51912&p=1. Letzter Aufruf: 09.08.2013.

[Hup-07] Hupp, H.; Dörsam, E.: Technische Universität Darmstadt, Deutschland: Verfahren zur messtechnischen Erfassung von einer auf einen Bedruckstoff aufgetragenen Farbschicht. Patentschrift DE 1020 0706 1899 B4, 2007.

[Hup-08] Hupp, H.: Qualitäts- und Prozesskontrolle gedruckter Interferenzeffektfarben erster Generation. Sierke Verlag, Göttingen: 2008.

[IBH-13] IBH Retail Consultants: Warensicherung. http://www.handelswissen.net/data/handelslexikon/lex_buchstabe.php?lex=w. Letzter Aufruf: 23.09.2013.

[ICC-06] ICC – International Chamber of Commerce: Anti-counterfeiting technology – A guide to Protecting and Authenticating Products and Documents. ICC, Barking (GB): 2006.

[ICT-13] ICT – Das Fraunhofer-Institut für Chemische Technologie: Holo-Impact. http://www.holo-impact.de. Letzter Aufruf: 23.09.2013.

[Imp-08] IMPULS Management Consulting: Global Spare Parts Management 2010. Studie. IMPULS Management Consulting GmbH, München: 2008.

[Imp-11] IMPULS Management Consulting: Den Serviceerfolg planen, steuern und messen. Ein Leitfaden für die Investitionsgüterindustrie. Vortrag: 13. Mai 2011. http://www.impuls-consulting.de/impuls/progof/datadocs/summary_serviceerfolg_planen_steuern_messen_final.pdf?PHPSESSID=bb506bf3905621e8b9ae2e4ca71d78c6. Letzter Aufruf: 12.11.2012.

[Inn-12] innovations-report: Mercer-Analyse "Service im Maschinenbau" / Ungenutzte Chancen im Servicegeschäft. IDEA TV Gesellschaft für kommunikative Unternehmensbetreuung mbH, Schmitten: 2012.

http://www.innovations-report.de/html/berichte/studien/bericht-23988.html. Letzter Aufruf: 12.11.2012.

[Ins-12] Institut für Produktionsmanagement, Technologie und Werkzeugmaschinen: ProOriginal. www.prooriginal.de. Letzter Aufruf: 08.11.2012.

[Ins-13] Institut für Umformtechnik und Umformmaschinen: Sinterbauteile sicher kennzeichnen und identifizieren. http://www.mm-logistik.vogel.de/verpackungstechnik/articles/198373. Letzter Aufruf: 22.01.2013.

[IPH-12] IPH – Institut für Integrierte Produktion Hannover: EZ-Pharm. www.ez-pharm.de. Letzter Aufruf: 08.11.2012.

[ISO15459-1] ISO/IEC 15459-1:2006: Informationstechnik. Eindeutige Identifikation. Teil 1: Eindeutige Identifikation von Transporteinheiten. International Organization for Standardization (ISO), Genf: 2006.

[ISO15459-2] ISO/IEC 15459-2:2006: Informationstechnik. Eindeutige Identifikation. Teil 2: Registrierungsverfahren. International Organization for Standardization (ISO), Genf: 2006.

[ISO15459-3] ISO/IEC 15459-3:2006: Informationstechnik. Eindeutige Identifikation. Teil 3: Allgemeine Regeln für die eindeutige Identifikation. International Organization for Standardization (ISO), Genf: 2006.

[ISO15459-4] ISO/IEC 15459-4:2008: Informationstechnik. Eindeutige Identifikation. Teil 4: Eindeutige Identifikation von Einzelelementen. International Organization for Standardization (ISO), Genf: 2008.

[ISO15459-5] ISO/IEC 15459-5:2007: Informationstechnik. Eindeutige Identifikation. Teil 5: Eindeutige Identifikation von Mehrweg-Transporteinheiten (RTIs). International Organization for Standardization (ISO), Genf: 2007.

[ISO15459-6] ISO/IEC 15459-6:2007: Informationstechnik. Eindeutige Identifikation. Teil 6: Eindeutige Identifikation von Produktgruppen. International Organization for Standardization (ISO), Genf: 2007.

[ISO15459-8] ISO/IEC 15459-8:2009: Informationstechnik. Eindeutige Identifikation. Teil 8: Bündelung von Transporteinheiten. International Organization for Standardization (ISO), Genf: 2009.

[ISO15962] ISO/IEC 15962:2013: Informationstechnik. Identifizierung von Waren mittels Hochfrequenz (RFID) für das Management des Warenflusses. Datenprotokoll: Regeln für die Datencodierung und Funktionen des logischen Datenspeichers. International Organization for Standardization (ISO), Genf: 2013.

[ISO15963] ISO/IEC 15963:2009: Informationstechnik. Artikelidentifizierung über Radiofrequenzen für das Managen des Warenflusses. Eindeutige Identifizierung von RF-Tags. International Organization for Standardization (ISO), Genf: 2009.

[ISO18000-6] ISO/IEC 18000-6:2013: Informationstechnik. Identifizierung von Waren mittels Hochfrequenz (RFID) fuer das Management des Warenflusses. Luftschnittstelle Parameter fuer die Kommunikation auf Frequenzen von 860-930 MHz. International Organization for Standardization (ISO), Genf: 2013.

[ISO18000-63] ISO/IEC 18000-63:2013: Informationstechnik. Identifizierung von Waren mittels Hochfrequenz (RFID) für das Management des Warenflusses. Parameter für die Kommunikation auf Frequenzen von 860-960 MHz Typ C. International Organization for Standardization (ISO), Genf: 2013.

[ISO9798-1] ISO/IEC 9798-1:2010: Informationstechnik. IT Sicherheitsverfahren. Authentifikation von Instanzen. Teil 1: Allgemeines Modell. International Organization for Standardization (ISO), Genf: 2010.

[ISO9798-2] ISO/IEC 9798-2:2008: Informationstechnik. IT-Sicherheitsverfahren. Authentifikation von Instanzen. Teil 2: Mechanismen auf Basis von Verschlüsselungsalgorithmen. International Organization for Standardization (ISO), Genf: 2008.

[ITP-13] IT-production.com : Produktpiraterie - Fälschern den Riegel vorschieben. Digitale Wächter de luxe. http://www.it-production

.com/index.php?seite=einzel_artikel_ansicht&id=52457. Letzter Aufruf: 12.08.2013.

[KIT-12a] KIT – Karlsruher Institut für Technologie: KoPira. www.ipek.uni-karlsruhe.de/kopira. Letzer Aufruf: 08.11.2012.

[KIT-12b] Karlsruher Institut für Technologie (KIT): www.produktionsforschung .de. Letzter Aufruf: 08.11.2012.

[Kle-10] Kleine, O.; Kreimeier, D.; Lieberknecht, N. (Hrsg.): Piraterierobuste Gestaltung von Produkten und Prozessen. Band 1 der Reihe „ Innovationen gegen Produktpiraterie“. VDMA Verlag GmbH, Frankfurt am Main: 2010.

[Kok-02] Kokot, J.: Spezialeffekte können unnachahmlich schön sein. Druckfarben und Lacke für Veredelung und Produktschutz. In: Deutscher Drucker (2002), Nr. 4, S. 30 - 33.

[Kok-11] Kokoschka, M.: Schutz vor Produktpiraterie jenseits juristischer Maßnahmen. Vortrag an der Industrie- und Handelskammer Chemnitz, 3. November 2011.

[Kor-09] Kornmeier, K.: Determinanten der Endkundenakzeptanz mobilkommunikationsbasierter Zahlungssysteme. Eine theoretische und empirische Analyse. Dissertation. Duisburg-Essen: Mercator School of Management. 2009.

[Kov-12] Kovács, N.; Bienert, R.; Oehlmann, H.; Schuermann, J.; Schmidt, E.; Walk, E.: RFID-Standardisierung im Überblick. Beuth, Berlin: 2012.

[Krä-06] Krämer, K.: Produktschutz – Basistechnologien, Entwicklungen und Möglichkeiten. In: Sokianos, N. (Hrsg.): Produkt- und Konzeptpiraterie. Erkennen, vorbeugen, abwehren, nutzen, dulden. S. 169 ff. Gabler, Wiesbaden: 2006.

[Krä-08] Krämer, K.: Produkt- und Markenschutz. Basistechnologien, St rategien und "Was kommt". In: Ident (2008) Nr. 1, S. 54-57.

[Krä-11] Krämer, K.: Produktschutz. Material- und Sendungsverfolgung – Vorgehen und Hinweise. In: ident Jahrbuch 2011. Ident Verlag & Service GmbH, Dortmund, S. 135 - 138.

[Kra-08] Krause, H.-U.; Arora, D.: Controlling-Kennzahlen – Key Performance Indicators. Zweisprachiges Handbuch Deutsch/Englisch. Bi-lingual Compendium German/English. Oldenbourg, München: 2008.

[Kro-06] Kroboth, D.: Präventionsmaßnahmen gegen Marken- und Produktpiraterie. Strategien für Unternehmen auf europäischer und internationaler Ebene. Shaker Verlag, Aachen: 2006.

[Krü-04] Krüger, R.; Vorbrüggen, J.; Picard, J.: Digitales Sicherheitsmerkmal für fälschungssichere Verpackung. Vortrag zur Tagung: Elektronische Geschäftsprozesse 2004, Universität Klagenfurt, 20.-21. September 2004.

[Krü-06] Krüger, J.; Nickolay, B.; Verhasselt, J. (Hrsg.); Klipfel, D.; Kamenz, C.; Vicente-Garcia, R.: Marken- und Produktpiraterie 2006. Wahrnehmung von Marken- und Produktpiraterie und Akzeptanz technologischer Schutzinstrumente. Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik (IPK), Berlin: 2006.

[Kuh-07] Kuhlmann, F.; Amende, M.: EPC-Informatioinsservices (EPCIS) und Umsetzung im EPC Showcase. Grundlageninformation. GS1 Germany GmbH, Köln: 2007.

[Lin-09] Lindemann, U.: Methodische Entwicklung technischer Produkte. Methoden flexibel und situationsgerecht anwenden. Springer, Berlin, Heidelberg: 2009.

[Lin-12] Lindemann, U.; Meiwald, T.; Petermann, M.; Schenkl, S.: Know-how-Schutz im Wettbewerb. Gegen Produktpiraterie und unerwünschten Wissenstransfer. Springer, Berlin, Heidelberg: 2012.

[Lou-13] Louisenthal: varifeye® Magic™ in Kasachstans 1000 Tenge Banknote. http://louisenthal-producton.s3.amazonaws.com/2010

/10/14/Ka sachstan_PL_Site%20deutsch-a5c9b744.pdf. Letzter Aufruf: 09.01.2013.

[Mac-10] Machatschke, M.: Deutsche Post DHL. Kunde statt Chaos. In: manager magazin. 40. Jahrgang (2010), August.

[Mak-13] Makita: Produktfälschungen. http://www.makita.de/uploads/media/Plagiate_01.pdf. Letzter Aufruf: 09.08.2013.

[Mal-05] Malik, H.; Schindler, S. (Hrsg.): Fälschungssichere Verpackungen. Sicherheitstechnologien und Produktschutz. Hüthig Verlag, Heidelberg: 2005.

[Mar-09] Marwan, P.: Original1: Die Fälschungsfahnder nehmen den Betrieb auf. ZDNet.de. 05.02.2009. http://www.zdnet.de/41526855/original1-die-faelschungsfahnder-nehmen-den-betrieb-auf. Letzter Aufruf: 14.02.2013.

[Mef-13] Meffert, H.; Burmann, C.; Koers, M. (Hrsg.): Markenmanagement. Identitätsorientierte Markenführung und praktische Umsetzung. Mit Best-practice-Fallstudien. Gabler, Wiesbaden: 2013.

[Mei-11] Meiwald, T.: Konzepte zum Schutz vor Produktpiraterie und unerwünschtem Know-how-Abfluss. Verlag Dr. Hut, München: 2011.

[Mei-13] Meiwald, T.: Schreiner Prosecure, Bruckmannring 22, 85764 Oberschleißheim. Experteninterview am 04.09.2013.

[Mer-06] Merkel, A.: Vortrag zur Eröffnung des Weltwirtschaftsforums 2006. Vortrag zur Tagung: World Economic Forum 2006, Davos, 25. Januar 2006.

[Mey-08] Meyer, G.; Främling, K.; Holmström, J.: Intelligent Products: a survey. Elsevier, Amsterdam: 2008.

[Mic-13] Microtrace, LLC. Taggant Technologies. http://microtracesolutions.com/taggant-technologies. Letzter Aufruf: 21.01.2013.

[Möh-12] Möhwald Unternehmensberatung: PiratPro. www.piratpro.de. Letzter Aufruf: 08.11.2012.

[MSDN-13a] MSDN: das Microsoft Developer Network. System.Security .Cryptography-Namespace. http://msdn.microsoft .com/de-de/library/System.Security.Cryptography.aspx. Letzter Aufruf: 14.08.2013.

[Mue-13] Müller, M.: HUECK FOLIEN Vertrieb und Service GmbH, Am Orthegelmühlbach 2a, 92637 Weiden. Gespräch am 08.01.2013.

[Mül-13] Müller Martini GmbH: MMServices Deutschland - Wir sind für Sie da! http://www.mullermartini.com/de/DesktopDefault.aspx/tabid-9589/8654_read-12066. Letzter Aufruf: 16.09.2013.

[Nee-07] Neemann, C.: Methodik zum Schutz gegen Produktimitationen. Shaker Verlag, Aachen: 2007.

[Neu-11] Neuhaus, S.: SSL und das BEAST. SSL-Server gegen BEAST-Angriffe härten. In: c't - magazin für computertechnik, Jahrgang 29 (2011) Nr. 23, S. 170.

[Nie-12] Niedling Wirtschaftsdienste GmbH: Produktpiraterie: Geklonte WC - Druckspüler, es gibt nichts was nicht kopiert wird! http://www.niedling-wirtschaftsdienste.de/de/Aktuelle_Meldungen/Aktuelle_Meldungen/site__232/content_news_detail__184/back_cont_id__232/limit_at__48. Letzter Aufruf: 08.11.2012.

[NIST-13] NIST – National Institute of Standards and Technology: Role Based Access Control (RBAC) and Role Based Security. http://csrc.nist.gov/groups/SNS/rbac. Letzter Aufruf: 24.08.2013.

[Nok-09] Nokia Corporation: Nokia 1616 Bedienungsanleitung. http://nds1.nokia.com/phones/files/guides/Nokia_1616_UG_de.pdf. Nokia GmbH, Bochum, 2009. Letzter Aufruf: 21.06.2013.

[OECD-08] OECD: Die wirtschaftlichen Folgen von Produkt- und Markenpiraterie. OECD, Paris: 2008.

[Oeh-10] Oehlmann, H.: ISO/IEC JTC 1/SC 31. Automatische Identifikation & Datenerfassung. Bericht über die kontinuierliche Normierung von Barcode & RFID. ehibcc, Peking, 28.05.2010. http://www.hibc.de

/Documente/10_ISO-Bericht-100916f_HIBC.pdf. Letzter Aufruf: 03.08.2013.

[Org-01] Orgalime aisbl: Wirksame Bekämpfung von Marken- und Produktpiraterie. Ein praktischer Leitfaden für die europäische Investitionsgüter-Industrie. Orgalime aisbl, Brüssel: 2001.

[Org-13] Orgeldinger, W.: Intelligente Transportverpackung. Tracking & Tracing von Mehrwegbehältern auf der Basis von Image Codes. http://www.logistik-heute.de/sites/default/files/logistik-heute/fachforen/lm_verpackung6.pdf. Letzter Aufruf: 08.08.2013.

[Par-12] Partners4Management: Original oder Fälschung? Kampf den Produktpiraten. http://www.muenchen.ihk.de/mike/ihk _geschaeftsfelder/ recht/Anhaenge/Vortrag-Produktpiraten -und-Internet.pdf. Letzer Aufruf: 08.11.2012.

[Pat-13] Patentanwaltskammer: Das Patent: Verdiente „Belohnung“ für Kreativität und Investitionen. http://www.patentanwalt.de/downloads /inn/ schutzrechtsarten/Deutsches_Patent.pdf. Letzter Aufruf: 31.05.2013.

[Pau-13] Paul, O.: Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 München. E-mail und Telefonat am 14.05.2013.

[Per-11] Perrey, J. ; Meyer, T.: Mega-Macht Marke. Erfolg messen, machen, managen. Redline-Verlag, München: 2005.

[Pet-08] Peters, B.: Hauni Maschinenbau AG, Kurt-A.-Körber-Chaussee 8-32, 21033 Hamburg. Expertengespräch am 08.05.2008.

[Pfa-07] Pfaff, G.: Spezielle Effektpigmente. Vinzentz Network GmbH, Hannover: 2007.

[Phy-13] Phys.Org / Medical Xpress: Microwires: replacement for the CD-ROM? http://phys.org/news3280.html. Letzter Aufruf: 17.01.2013.

[Pol-13] Polysecure GmbH: Widerstandsfähigkeit. http://www.polysecure .eu/deutsch/anwendung/widerstandsfaehigkeit.html. Letzter Aufruf: 09.01.2013.

[Pri-13] Printcolor: Lumineszenzeffekte im Siebdruck. http://de.printcolor.ch/ pdf/Lumineszenzfarben.pdf. Letzter Aufruf: 07.01.2013.

[Pro-09] ProAuthent: Integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. Vortrag durch Grüneis, B.: Analyse der rechtlichen Rahmenbedingungen für ein Schutzsystem. 5. Projekttreffen 2009, Technische Univerisät München, 28. Januar 2009, nicht öffentlich.

[Pro-12] Produktpiraterie.org: Plattform für Produkt- und Markenschutz sowie Geräte- und Produktsicherheit. http://www.produktpiraterie .org. Letzter Aufruf: 18.12.2012.

[Pro-13a] PROCESS: Eindeutige Authentifizierung ohne Markierung bei Pharmaprodukten. http://www.process.vogel.de/logistik _verpackung/verpackungstechnik/articles/63183. Letzter Aufruf: 21.01.2013.

[Pro-13b] prozesstechnik online: Digitale Kopierschutzlösung. http://www.prozesstechnik-online.de/test/-/article/31534493/32089508/Digitale-Kopierschutzl%C3%B6sung/art_co_INSTANCE_0000/maximized. Letzter Aufruf: 21.02.2013.

[Pub-10] publish-industry Verlag GmbH: Funketiketten steuern die Fertigung. Die für Logistik und Handel entwickelte UHF-Technologie Einzug in die Fabrikhallen. In: A&D Kompendium 2009/2010. publish-industry Verlag GmbH, München: 2010. http://www.aud24 .net/pi/index.php?StoryID=189&articleID=163971. Letzter Aufruf: 13.08.2013.

[Ran-08] Rankl, W.; Effing, W.: Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards. Carl Hanser, München: 2008.

[Rat-13] Rat der Europäischen Union: Glossar. Sicherheitsdokumente, Sicherheitsmerkmale und andere einschlägige Fachbegriffe. http://prado.consilium.europa.eu/de/glossarypopup.html. Letzter Aufruf: 08.01.2013.

[Rav-01] Ravikanth, P. S.: Physical One-Way Functions. Massachusetts Institute of Technology, Cambridge: 2001.

[Rec-08] Recher, W.: MULTIVAC Sepp Haggenmüller GmbH & Co. KG, Bahnhofstr. 4, 87787 Wolfertschwenden. Expertengespräch am 07.05.2008.

[Red-13] Rediska – Technische Konzeption und Programmierung: Hochsicherheitssteaks beim Netto Marken-Discount in Berlin. http://rediska.de/hochsicherheitssteaks-beim-netto-marken-discount-in-berlin. Letzter Aufruf: 17.01.2013.

[Rei-10] Reinhart, G.: Fabrikplanung. Vorlesungsskriptum: Institut für Werkzeugmaschinen und Betriebswissenschaften. Technische Universität München: 2010.

[RFI-13a] RFIDTags.com: SMARTRAC HF RaceTrack RFID Tag. http://www.rfid tags.com/smartrac-racetrack-rfid-tag. Letzter Aufruf: 19.07.2013.

[RFI-13b] RFID&CARD Technology (Shenzhen) Co., Ltd.: LF RFID Glass Tube. http://www.tradevv.com/chinasuppliers/rfidandcard _p_159d54/china-Glass-Tube-Animal-Tag-LF-RFID-Glass-Tube.html. Letzter Aufruf: 19.07.2013.

[Rhe-13] Rhein-Main-Verkehrsverbund GmbH: DB-Kooperationsfahrkarten. www.rmv.de. Letzter Aufruf: 05.03.2013.

[Ric-08] Richter, C.: MTU Aero Engines GmbH, Dachauer Straße 665, 80995 München. Expertengespräch am 10.10.2008, E-Mail des 04.06.2013.

[Röß-13] Rößler, M.: Test: Die günstigsten Drucker aller Klassen. Über 1.300 Euro sparen. http://www.chip.de/artikel/Test-Die-guenstigsten-Drucker -aller-Klassen_37340926.html. Letzter Aufruf: 13.02.2013.

[Rot-00] Rother, M.; Shook, J.: Sehen Lernen. Mit Wertstromdesign die Wertschöpfung erhöhen und Verschwendung beseitigen. Deutsche Ausgabe des LOG X Verlag, Stuttgart: 2000.

[Rot-05] Roth, T.: Informationssicherheitsverfahren von RFID-Transpondern. In: OBJEKTspektrum. 12. Jahrgang (2005), Online Themenspecial RFID. www.sigs-datacom.de/fileadmin/user_upload/zeitschriften /os/2005/RFID/roth_OS_rfid_05.pdf. Letzter Aufruf: 12.08.2013.

[Rup-07] Rupp, C.; Queins, S.; Zengler, B.: UML 2 Glasklar. Praxiswissen für die UML-Modellierung. Carl Hanser, München: 2007.

[Sam-12] sammyacc1: Produktpiraterie Intralogistik_2012.mov. http://www.youtube.com/watch?v=0rU0zmcEW68. Letzter Aufruf: 06.11.2012.

[Sar-00] Sarma, S.; Brock, D.; Ashton, K.: The Networked Physical World. Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification. MIT Auto-ID Center, Massachusetts Institute of Technology, Cambridge: 2000.

[Sch-06] Schneier, B.: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Pearson Studium, München: 2006.

[Sch-08] Schindler, S.: We care for your brand. Innovative Hightech-Lösungen für Produkt- und Markenschutz. Vortrag zur Tagung: 6. APM-Kongress 2008, IHK-Akademie München, 15. April 2008.

[Sch-10a] Schnapauff, K.: Präventiver Nachahmungsschutz bei technischen Produkten für industrielle oder professionelle Anwendungen. TCW Transfer-Centrum für Produktions-Logistik und Technologie-Management, München: 2010.

[Sch-10b] Schwenk, J.: Sicherheit und Kryptographie im Internet. Von sicherer E-Mail bis zu IP-Verschlüsselung. Vieweg+ Teubner, Wiesbaden: 2010.

[Sch-10c] Schmidt-Riediger, B.: Schreiner Prosecure, Bruckmannring 22, 85764 Oberschleißheim. Expertengespräche mit Erarbeitung eines Gesamtergebnisses am 23.03.2010.

[Sch-13a] Schreiner Group GmbH & Co. KG.: Sicher ist sicher. http://www .schreiner-prosecure.com/index.php?id=2294&L=0. Letzter Aufruf: 17.01.2013.

[Sch-13b] Schreiner Group GmbH & Co. KG.: Sechs Lagen Schutz. Ein integriertes Label. Unzählige Möglichkeiten. http://www.schreiner-medipharm.com/0/produktloesungen/pharma-security/secumed. Letzter Aufruf: 13.05.2013.

[Sch-13c] Schreiner Group GmbH & Co. KG.: Track-and-Trace-Lösung zur Produktauthentifizierung. http://www.schreiner-prosecure.com /index.php ?id=2140&L=0. Letzter Aufruf: 20.06.2013.

[Sch-13d] Schreiner Group GmbH & Co. KG.: Markenschutz in Gips gegossen. http://www.schreiner-prosecure.com/index.php ?id=2138&L=0. Letzter Aufruf: 20.06.2013.

[Sec-12] securPharm e.V.: Regeln zur Codierung verifizierungspflichtiger Arzneimittel im deutschen Markt zum Schutz vor Arzneimittelfälschungen. securPharm e.V., Frankfurt am Main: 2012.

[Sec-13] securPharm e.V.: Der deutsche Schutzschild gegen Arzneimittelfälschungen. http://www.securpharm.de. Letzter Aufruf: 01.03.2013.

[Shr-13] Shriram Veritech Solutions PVT. LTD.: Security Features. http://www.veritechindia.com/securityfeatures.html#mydiv7. Letzter Aufruf: 21.01.2013.

[Sie-13a] Siegrist, H.: Geschichte des geistigen Eigentums und der Urheberrechte. Kulturelle Handlungsrechte in der Moderne. http://www.uni-leipzig.de/~kuwi/siegrist/Siegrist_in_Hofmann.pdf. Letzter Aufruf: 23.01.2013.

[Sie-13b] Siemens AG Competence Center RFID: Den Fälschern auf der Spur. RFID als wirksames Mittel gegen Produktpiraten. http://www.competence-site.de/industrielle-sicherheitstechnik /Produkte-und-Marken-schuetzen. Letzter Aufruf: 12.08.2013.

[Sil-08] da Silva, J.; Hoppen, K.; Vogt, R.: Piraten einen Schritt voraus. In: Materialfluss Markt 2008. 40. Jahrgang (2008), Dezember, S. 82-83.

[Sim-13] Simons, R.: 3S GmbH, Lise-Meitner-Str. 6, 48301 Nottuln. Gespräch am 05.08.2013.

[Sit-06] Sitte, B.: Schutzmaßnahmen gegen chinesische Produkt- und Markenpiraterie. Diplomica GmbH, Hamburg: 2006.

[Sky-13] SkyRFID Inc.: RFID Gen 2 - What is it? - Smart RFID! http://www.skyrfid.com/RFID_Gen_2_What_is_it.php. Letzter Aufruf: 02.08.2013.

[Sok-06] Sokianos, N.: Produkt- und Konzeptpiraterie erkennen, vorbeugen, abwehren, nutzen, dulden. Gabler, Wiesbaden: 2006.

[Spr-12] Springer Gabler: Gabler Wirtschaftslexikon - Die ganze Welt der Wirtschaft. Ware. Springer Gabler | Springer Fachmedien Wiesbaden GmbH. www.wirtschaftslexikon.gabler.de. Letzter Aufruf: 05.11.2012.

[Spr-13] Springer Gabler: Gabler Wirtschaftslexikon - Die ganze Welt der Wirtschaft. Supply Chain Management. Springer Gabler | Springer Fachmedien Wiesbaden GmbH. www.wirtschaftslexikon.gabler.de. Letzter Aufruf: 19.08.2013.

[Sta-07] Staake, T.: Counterfeit Trade – Economics and Countermeasures. Difo-Druck, Bamberg: 2007.

[Sta-08] Staake, T.; Fleisch, E.: Countering Counterfeit Trade. Illicit Market Insights, Best-Practice Strategies, and Management Toolbox. Springer, Berlin, Heidelberg: 2008.

[Ste-08] Steinebach, M.; Liu, H.: Digitale Wasserzeichen zum Schutz analoger Güter. In: Industrie Management. Zeitschrift für industrielle Geschäftsprozesse. 24. Jahrgang (2008) Nr. 6. S. 55-58.

[Ste-09] Sterbak, R.: Nur echt mit dem Chip. Digitale Wächter | RFID-Chips. In: Siemens AG. Pictures oft he Future. Die Zeitschrift für Forschung und Innovation. 8. Jahrgang (2009), Frühjahr. S. 45-47.

[Ste-11a] Stephan, M.; Schneider, M.: Marken- und Produktpiraterie. Fälscherstrategien, Schutzinstrumente, Bekämpfungsmanagement. Symposion Publishing, Düsseldorf: 2011.

[Ste-11b] Steiner, P.: Sensory Branding. Grundlagen multisensualer Markenführung. Gabler Verlag, Wiesbaden: 2011.

[Sto-10] Stooß, R.: Schreiner Prosecure, Bruckmannring 22, 85764 Oberschleißheim. Expertengespräche mit Erarbeitung eines Gesamtergebnisses am 23.03.2010.

[Sto-11] Stockenberger, D.: Grundlagen der RFID-Software, Datenmodell. Vortrag zur Tagung: 10. VDA-Praxisforum Logistik 2011, Verband der Automobilindustrie e. V. (VDA), Behrenstr. 35, 10117 Berlin: 14. Juli 2011.

[Sto-12] Stockenberger, D.; Durchholz, J.; Günthner, W.: Integrierte Sicherheitsmerkmale als Schutz vor Produktpiraterie im Maschinen- und Anlagenbau. http://www.logistics-journal.de/not-reviewed/2011/11/ 3153/stockenberger.pdf. Letzter Aufruf: 15.11.2012.

[Sto-13] Stop Piracy: Bildergalerie. Ein Einblick in die Welt der Fälschungen, der perfekten Kopien und Vernichtungsaktionen. http://www.stop-piracy.ch/de/candp/cap70.shtm. Letzter Aufruf: 09.08.2013.

[Swo-08] Swoboda, J.; Spitz, S.; Pramateftakis, M.: Kryptografie und IT-Sicherheit. Grundlagen und Anwendungen. Vieweg & Teubner, Wiesbaden: 2008.

[Tai-13] Tailorlux GmbH: Tailorlux – Intelligent Materials. http://www.tailorlux .com. Letzter Aufruf: 17.01.2013.

[Tan-08] Tanenbaum, A.; von Steen, M.: Verteilte Systeme. Prinzipien und Paradigmen. Pearson Studium Education, München: 2008.

[Tec-12] Technische Universität Kaiserslautern: KoPiKomp. www.kopikomp.de. Letzter Aufruf: 08.11.2012.

[Tec-13] TEC-IT Datenverarbeitung GmbH: Online Barcode Generator. http://barcode.tec-it.com/barcode-generator.aspx?LANG=de. Letzter Aufruf: 19.07.2013.

[Tes-13] Tesa Scribos GmbH: tesa Holospot® – Bewährter Fälschungsschutz und effektive Produktverfolgung. http://www.tesa-scribos.com/deu /security_technology/tesa_holospot. Letzter Aufruf: 17.01.2013.

[Tho-13] Thoss, F.: Verband Forschender Arzneimittelhersteller e.V., Hausvogteiplatz 13, . Gespräch am 28.02.2013.

[Thu-13] Thul, U.: DB Vertrieb GmbH (P.DVO 11), Frankenallee 2-4, 60327 Frankfurt. E-mail des 18.06.2013.

[Tra-13] Tradeinde.com: Bibliothek Em Etikett. http://www.tradeinde.com /product-eas-system/library-em-label-387234.html. Letzter Aufruf: 17.01.2013.

[Tre-13] Trebus, J.; Parus, P.: Tracking & TracingSysteme. in Wertschöpfungsnetzwerken Rückverfolgbarkeit mit Hilfe von RFID. www.leibniz-institut.de/cms/pdf2/trebus_tracking_tracing_systeme .pdf. Letzter Aufruf: 08.08.2013.

[Tro-10] Troeger, R.; Alt, R.: Service-oriented Supply Chain Event Management – A Case Study from the Fashion Industry. In: Abramowicz, W.; Alt, R.; Fähnrich, K.-P.; Franczyk, B.: Maciaszek, L. (Hrsg.): Informatik 2010. Business Process and Service Science. Tagungsband der ISSS/BPSC 2010, Leipzig, 27. September 2010.

[Trö-11] Tröger, R.; Alt, R.: Serviceorientiertes SCEM. Nutzen und Architektur für globale Lieferketten am Beispiel der Modeindustrie. In: Bogaschewsky, R.; Eßig, M.; Lasch, R.; Stölzle, W. (Hrsg.): Supply Management Research. Aktuelle Forschungsergebnisse 2011. Gabler Verlag | Springer Fachmedien, Wiesbaden: 2011. S. 255 - 265.

[TUM-13] TUM – Technische Universität München: Download von Logos und Vorlagen. http://portal.mytum.de/corporatedesign/download /index_html. Letzter Aufruf: 23.09.2013.

[Uli-09] Ulisch, A.: Protexxion. Einsatzmöglichkeiten für die mittelständische Industrie. Vortrag beim Presse-Workshop der LOG mbH:

Supply Chain und Produktpiraterie – Innovation im Bereich fälschungssichere Kennzeichnung und mobile Authentifizierung von Produkten, Bonn, 05. - 06.11.2009.

[Ulr-76] Ulrich, P.; Hill, W.: Wissenschaftstheoretische Grundlagen der Betriebswirtschaftslehre (Teil II). In: Wirtschaftswissenschaftliches Studium. Zeitschrift für Ausbildung und Hochschulkontakt, 5. Jahrgang (1976) Heft 8, S. 345-350.

[Uni-04] United States District Court, Entscheidung 29.07.2004, Aktenzeichen CV-03-3787(SIF)(WDW), Fagan vs. Amerisourcebergen Corp. and others.

[Uni-12] Universität Potsdam, Lehrstuhl für Wirtschaftsinformatik und Electronic Government: PROTACTIVE. www.knowledge-firewall.de. Letzter Aufruf: 08.11.2012.

[Unt-12] Unterstein, M.; Matthiessen, G.: Relationale Datenbanken und SQL in Theorie und Praxis. Springer, Berlin: 2012.

[VDI2693] VDI-Richtlinie 2693, Blatt 1: Investitionsrechnung bei Materialfluß-planungen mit Hilfe statischer und dynamischer Rechenverfahren. Verein Deutscher Ingenieure, Düsseldorf: 1996.

[VDI4416] VDI-Richtlinie 4416: Betriebsdatenerfassung und Identifikation. Identifikationssysteme. Deutscher Ingenieure, Düsseldorf: 1998.

[VDMA-11] VDMA Betriebswirtschaft: VDMA-Kennzahlen Kundendienst 2010 - vergleichen, verstehen, verändern. VDMA, Frankfurt am Main: 2011.

[VDMA-12a] VDMA Produkt- und Know-how-Schutz: VDMA Studie Produktpiraterie 2012. VDMA, Frankfurt am Main: 2012.

[VDMA-12b] VDMA: Flagge hissen gegen Produktpiraten – Mit High Tech gegen Technologieklau. http://www.vdma-webbox.tv/deutsch/filmdaten bank/ flagge-hissen-gegen-produktpiraten-mit-high-tech-gegen-technologie klau.html. Letzter Aufruf: 16.11.2012.

[Ver-05] Verisign Inc.: The EPCglobal Network: Enhancing the Supply Chain. VeriSign Inc., Reston, USA: 2005.

[Ver-08] Verisign Inc.: EPCglobal Network Architecture Overview. VeriSign Inc., Reston, USA: 2008.

[Vis-12] Visality Consulting GmbH: After Sales Management / Life Cycle Management. Herausforderungen im After Sales und Life Cycle Management. http://www.visality.de/aftersales_lifecycle.html. Letzter Aufruf: 12.11.2012.

[Völ-10] Völcker, T.: Schreiner Prosecure, Bruckmannring 22, 85764 Oberschleißheim. Expertengespräche mit Erarbeitung eines Gesamtergebnisses am 23.03.2010.

[Völ-13] Völcker, T.: Einsatz innovativer Sicherheitstechnologien für den effektiven Produkt- und Markenschutz. http://www.muenchen.ihk.de/de/recht/Anhaenge/Vortrag-Schutz-mit-Sicherheitstechnologie.pdf. Letzter Aufruf: 08.01.2013.

[Vor-09] Vorbrüggen, J.: Schreiner Prosecure, Bruckmannring 22, 85764 Oberschleißheim. E-mail des 19.08.2009.

[Wal-05] Walther, T; Kaufmann, M.: Marken- und Produktfälschung – das Verbrechen des 21. Jahrhunderts. MAN Roland Druckmaschinen AG, Offenbach: 2005.

[Web-07] Weber, W.: Zutrittskontrolle während der FIFA WM 2006. In: In: Ident (2007) Nr. 1, S. 21.

[Wei-12] Weinländer, M.: Varianten im Griff. UHF-RFID für durchgängige Steuerung von Produktion und Logistik. http://www.automation.siemens.com/wcmsnewscenter/details.aspx?xml=/content/10001666/de/gc/Pages/FAV-253-2012-IA-SC-221-12.xml&xsl=publication-de-www4 .xsl. Letzter Aufruf: 25.07.2013.

[Wel-07] von Welser, M.; González, A.: Marken- und Produktpiraterie. Strategien und Lösungsansätze zu ihrer Bekämpfung. Wiley-VCH, Weinheim: 2007.

[Wib-12] WIBU-SYSTEMS AG: Pro-Protect. www.pro-protect.de. Letzter Aufruf: 08.11.2012.

[Wie-11] Wienholdt, H.: Dynamische Konfiguration der Ersatzteillogistik im Maschinen- und Anlagenbau. Apprimus Wissenschaftsverlag, Aachen: 2011.

[Wie-12] Wiechers, R.; Schneider, G.: Maschinenbau in Zahl und Bild 2012. VDMA, Frankfurt am Main: 2012.

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

[Wil-11] Wildemann, H.: Produktpiraterie & Nachahmungen. Betriebswirtschaftliche Elemente eines integrativen Schutzsystems. TCW Transfer-Centrum GmbH & Co. KG, München: 2011.

[Win-07] Winkler, I.; Wang, X.: Made in China – Marken- und Produktpiraterie. Strategien der Fälscher und Abwehrstrategien für Unternehmen. Verlag für Interkulturelle Kommunikation, Frankfurt am Main: 2007.

[Win-13] Winzenried, O.; Neifer, W.: Pro-Protect. Produktpiraterie verhindern mit Softwareschutz. http://www.pro-protect.de/1/index.php?id=presse. Letzter Aufruf: 09.08.2013.

[Wöh-05] Wöhe, G.; Döring, U.: Einführung in die Allgemeine Betriebswirtschaftslehre. Franz Vahlen, München: 2005.

[Wör-13] Wörner Verlag: Hundertwasser Kunstdruck. http://www.hundertwasser-kalender.de/Hundertwasser-Kunstdruck-886-Geburt-eines-Automobils. Letzter Aufruf: 21.01.2013.

[WTO-12] World Trade Organization: Time Series on international trade. http://stat.wto.org/StatisticalProgram/WSDBStatProgramHome.aspx?Language=E. Letzter Aufruf 30.10.2012.

[Wur-11] Wurzer, A.; Kaiser, L. (Hrsg.): Handbuch Internationaler Know-how-Schutz. Bundesanzeigerverlag, Köln: 2011.

[ZDF-08] ZDF: Produktpiraterie. Original und Fälschung. http://www.zdf.de/ZDFmediathek/content/Produktpiraterie_Original_und_Faelschung/810/129262. Letzter Aufruf: 26.05.08.

[Zim-13] Zimmermann, L.: II. Unternehmerischer Patriotismus im Zeitalter der Globalisierung. http://www.herbert-quandt-stiftung.de/II_Unternehmerischer_Patriotismus_im_Zeitalter_der_Globalisierung. Letzter Aufruf: 04.06.2013.

[Zit-12] Zitate-Online.de: http://www.zitate-online.de/literaturzitate/allgemein/2362/der-mensch-hat-dreierlei-wege-klug-zu-handeln.html. Letzter Aufruf: 31.10.2012.

12 Abbildungsverzeichnis

12.1 Abbildungsverzeichnis Hauptteil

12.2 Abbildungsverzeichnis Anhang

13 Tabellenverzeichnis

13.1 Tabellenverzeichnis Hauptteil

13.2 Tabellenverzeichnis Anhang

Anhang A Sicherheitsmerkmale in Form eines Kennzeichens, einer Technologie oder eines Systems

In diesem Anhang werden aktuelle Sicherheitsmerkmale beschrieben. Diese Übersicht ist Ergebnis einer umfangreichen Recherche. Es wurden 85 verschiedene Quellen analysiert und dabei 68 verschiedene Technologien herausgearbeitet. Diese 68 Technologien sind im Folgenden einzeln beschrieben und die dafür ausgewerteten Quellen angegeben. Die Quellenangaben zeigen auf, wo Angaben zu den jeweiligen Technologien zu finden sind und dienen insbesondere auch dazu, dass der Leser sich weiter informieren kann. Sofern verfügbar sind bei den Beschreibungen auch Beispiele und aussagekräftige Bilder angefügt.

Dieser Katalog an Sicherheitsmerkmalen und -technologien ist der aktuell umfangreichste für die produzierende Industrie. Dennoch erhebt der Katalog keinen Anspruch auf Vollständigkeit, da es in diesem Bereich permanent Neuentwicklungen gibt [Bun-13a, EZB-13a]. Zudem wurden Technologien, die insbesondere zur Sicherung der Integrität von Verpackungen entwickelt wurden, nicht aufgenommen. In Tabelle 3-1, S. 39 sind sämtliche, hier beschriebenen Technologien gelistet und in passende Kategorien eingeordnet. Diese Tabelle wird hier der Übersichtlichkeit halber wiederholt.

Tabelle A-1: Sicherheitsmerkmale in Form eines Kennzeichens, einer Technologie oder eines Systems, Wiederholung der Tabelle 3-1

Klasse	Gruppe	Kennzeichen / Technologie / System	Abschnitt
Biologisch	-	Antikörper	A.1.1
		Desoxyribonukleinsäure (DNA)	A.1.2
		DNA-Sequenz	A.1.2.1
		DNA-Strang	A.1.2.2
Chemisch	-	Nanotech Barcode	A.2.1
Elektrisch / magnetisch / elektromagnetisch	-	Akustomagnetisches Etikett	A.3.1
		Elektromagnetisch detektierbare Farbe	A.3.2
		Elektromagnetisches Etikett	A.3.3
		Elektromagnetische Glasfasern	A.3.4
		Mikrochip mit Kontakt	A.3.5
		Radiofrequenzidentifikation (RFID)	A.3.6
Haptisch	**Druckverfahren**	Hochdruck	A.4.1.1
		Matrixdruck / Nadeldruck	A.4.1.2
		Tiefdruck	A.4.1.3
		Intagliodruck / Stichtiefdruck	A.4.1.3.1
		Orlof-Technik / Schabloneneinfärbetechnik	A.4.1.3.2
		Rastertiefdruck	A.4.1.3.3
		Siebdruck	A.4.1.4
	Prägen	Blindprägung	A.4.2.1
		Heißfolienprägung	A.4.2.2

Klasse	Gruppe	Kennzeichen / Technologie / System	Abschnitt
Optisch	**Optische Effekte**	Durchsichtsfenster	A.5.1.1
		Foliendurchsichtsfenster	A.5.1.1.1
		Moiré Magnifier-Element	A.5.1.1.2
		Durchsichtsregister	A.5.1.2
		Hologramme	A.5.1.3
		Laserkippbild	A.5.1.4
		Parallaxe	A.5.1.5
		Retroreflektierende Folie	A.5.1.6
		Wasserzeichen	A.5.1.7
	Pre-Press-Druckmerkmale	Anti-Kopier-Muster	A.5.2.1
		Besondere Schriftart	A.5.2.2
		Digitale Wasserzeichen	A.5.2.3
		Mikrotext	A.5.2.4
		Rasterbild	A.5.2.5
		Scrambled image / codiertes Bild	A.5.2.6
	Spezialdruck	Guillochen	A.5.3.1
		Irisdruck / Regenbogendruck	A.5.3.2
	Spezialfarben / Spezialpartikel	Clustermerkmal	A.5.4.1
		Fotochrome Farbe	A.5.4.2
		Reversible fotochrome Farbe	A.5.4.2.1
		Irreversible fotochrome Farbe	A.5.4.2.2
		Fluoreszenz	A.5.4.3
		Infrarot-Farbe (IR)	A.5.4.3.1
		Röntgenlumineszenz	A.5.4.3.2
		Tagesleuchtfarbe / Neonfarbe als Echtfarbelement	A.5.4.3.3
		Ultraviolette Farbe (UV)	A.5.4.3.4
		Interferenz- und Effektfarbe	A.5.4.4
		Kippfarbe / optisch variable Druckfarbe	A.5.4.5
		Magnetisierbare Farbe	A.5.4.6
		Metallreagenzfarbe	A.5.4.7
		Metamere Farbe	A.5.4.8
		Mikrofarbcode	A.5.4.9
		Mikropunkte	A.5.4.10
		Pen-Reactive-Ink / Reagenzfarbe	A.5.4.11
		Phosphoreszenz	A.5.4.12
		Sicherheitsfärbemittel	A.5.4.13
		Sonderfarbe	A.5.4.14
		Spektralsensible Farbe	A.5.4.15
		thermoreaktive Farbe	A.5.4.16
		Thermische Pigmente	A.5.4.16.1
		Thermochrome Pigmente	A.5.4.16.2
	Sonstige	Feuchtstempelabdruck	A.5.5.1
		Lasergravur	A.5.5.2
		Oberflächenauthentifizierung	A.5.5.3
		Musteroberfläche	A.5.5.3.1
		Sprengprägen	A.5.5.3.2
		Stochastische Schwankungen im Fertigungsprozess	A.5.5.3.3
		Perforation	A.5.5.4
		Laserperforation	A.5.5.4.1
		Nadelperforation	A.5.5.4.2
		Rauschmustercodes	A.5.5.5
		Sicherheitsanstanzung	A.5.5.6
		Sicherheitsfaden	A.5.5.7
Sonstige	-	Duftstoffe	A.6.1
		Markierung pulvermetallurgisch hergestellter Bauteile	A.6.2
		Nanopartikel	A.6.3

A.1 Biologische Sicherheitsmerkmale

A.1.1 Antikörper

Das als Spezialfarbe aufzubringende Markermaterial beinhaltet Biomoleküle (Antigene). Diese reagieren nach einem Schlüssel-Schloss-Prinzip mit den passenden Antikörpern. Die Authentifizierung findet mit einem Färbe-Schnelltestverfahren statt.

Quellen: Hop-03, Hot-11, ICC-06, Kok-02, Sit-06

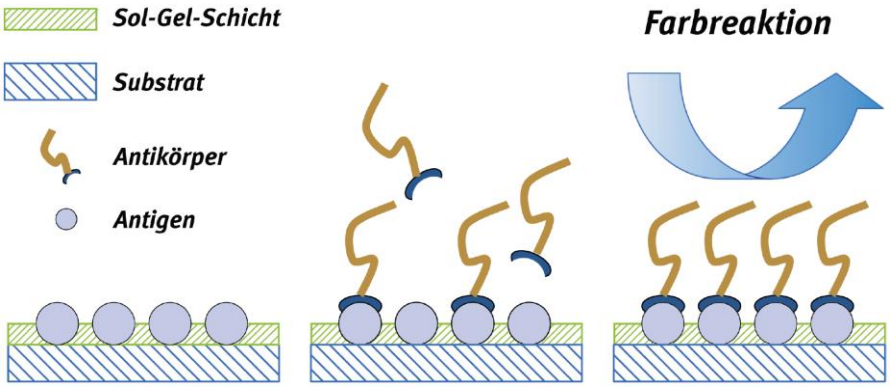


Abbildung A-1: Antigene reagieren mit Antikörpern in einem Färbe-Schnelltestverfahren [Hot-11]

A.1.2 Desoxyribonukleinsäure

Für künstliche Desoxyribonukleinsäure (DNA) werden die vier Bestandteile Adenin, Thymin, Cytosin und Guanin je DNA-Tinktur wahlfrei kombiniert. Bei der Verknüpfung der vier Bausteine ergibt sich aufgrund der enormen Vielfalt ein unverwechselbares Merkmal. DNA kann, wie im Folgenden dargestellt, auf zwei verschiedene Weisen zur Anwendung kommen.

A.1.2.1 DNA-Sequenz

Authentifizierung von DNA durch Auswertung der Sequenzen im Labor.

Quellen: Beh-13a, Mal-05, Wel-07

Abbildung A-2: Auswertung von DNA [Hei-13]

A.1.2.2 DNA-Strang

Nach Erzeugung einer DNA-Sequenz wird diese in die beiden Stränge zerlegt. Ein Trägermedium beinhaltet den einen der beiden Stränge und wird auf dem zu markierenden Produkt aufgebracht. Eine Testflüssigkeit enthält den anderen der beiden Stränge. Nach Aufbringen der Testflüssigkeit auf das Trägermedium reagieren die beiden Stränge und bilden einen Doppelstrang, sofern die beiden DNA-Stränge zusammengehören. Nach dieser sogenannten Hybridisierung beginnt das System innerhalb weniger Sekunden zu leuchten. Dieses Leuchten wird mit einem Scanner erfasst und der Nachweis erbracht, dass das Produkt echt ist.

Beispiel: brandprotection

Quellen: Boc-13, Fuc-06, Mal-05, Mei-11, Pro-12, Sit-06, Völ-13

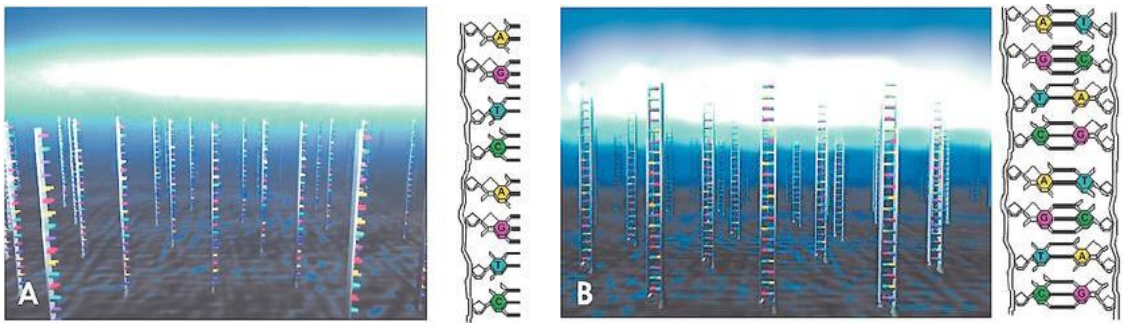


Abbildung A-3: DNA-Einzelstränge (links) und DNA-Doppelstränge nach der Hybridisierung mit einer komplementären DNA [Boc-13]

A.2 Chemische Sicherheitsmerkmale

A.2.1 Nanotech Barcode

Gruppe von Molekülen, die bei Belichtung mit einer speziellen Licht-Frequenz ein einzigartiges individuelles Licht-Spektrum emittiert, das mit einem digitalen Handlesegerätes überprüft wird. Die Integration ist in die meisten industriell hergestellten Materialien (Polymere, Papier, Metall, etc.) möglich.

Beispiele: DataTraceDNA (Digital Nanoparticel Authentication)

Quellen: Dat-13a, Krü-06

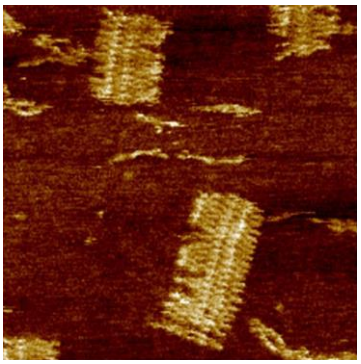


Abbildung A-4: Authentifizierung mittels DatatraceDNA [Krü-06]

A.3 Elektrische / magnetische / elektromagnetische Sicherheitsmerkmale

A.3.1 Akustomagnetisches Etikett

Die akustomagnetischen Etiketten enthalten einen amorphen Metallstreifen als Sensorkomponente. Das Etikett ist im magnetisierten Zustand aktiviert, im entmagnetisierten Zustand deaktiviert. Der Metallstreifen ist frei beweglich gelagert und dient als Resonator. Im aktivierten Zustand wird dieser im Detektionsbereich durch einen Magnetfeldimpuls im Ultraschallbereich (58 kHz) zum Schwingen angeregt. Da dies der Resonanzfrequenz des Plättchens entspricht, beginnt dieses zu schwingen. Dieses Schwingen hält nach Anregung etwas 5ms an und erzeugt einen magnetischen Impuls, der detektierbar ist.

Beispiel: Diebstahlsicherung im Einzelhandel

Quellen: Art-13, Red-13

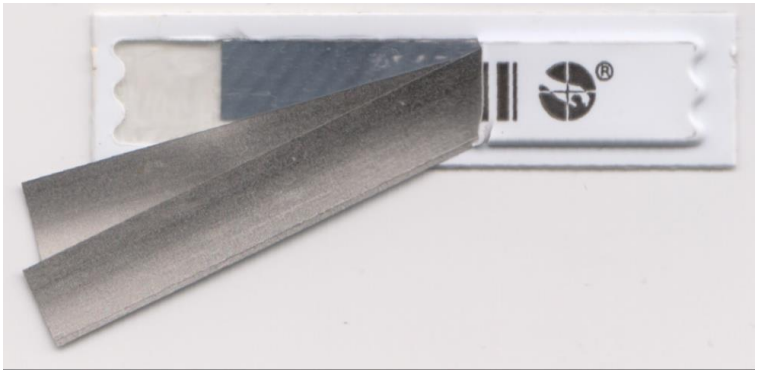


Abbildung A-5: Akustomagnetisches Etikett [Red-13]

A.3.2 Elektromagnetisch detektierbare Farbe

Diese elektromagnetischen Markierungen können auch an verdeckten Stellen berührungslos erkannt werden, beispielsweise eine versteckte Anbringung im Klebefalz einer Verpackung.

Quellen: Kok-02

A.3.3 Elektromagnetisches Etikett

Dieses Etikett enthält reversibel aktivierbare Metallstreifen einer leichtmagnetisierbaren Legierung. Diese erzeugt im elektromagnetischen Wechselfeld leicht nachweisbare Oberschwingungen.

Beispiel: Bücherei, Diebstahlsicherung im Einzelhandel

Quellen: Hop-03

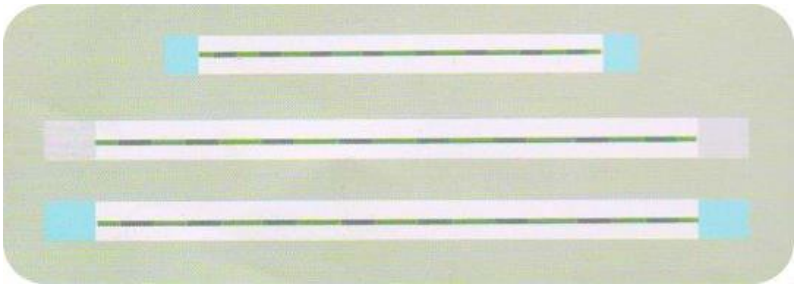


Abbildung A-6: Drei elektromagnetische Etikette [Tra-13]

A.3.4 Elektromagnetische Glasfasern

Diese feinen, 10 bis 50 µm dicken Glasfasern mit einem Kern aus amorphem Metall sind elektromagnetisch kodierbar und mit elektronischen Prüfgeräten erfassbar.

Beispiel: MicroWire®

Quellen: Cor-13, Gün-11a

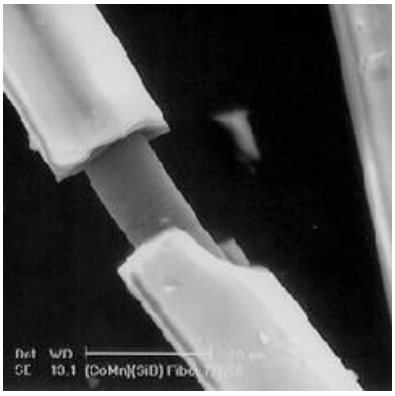


Abbildung A-7: Microwires [Phy-13]

A.3.5 Mikrochip mit Kontakt

Integrierte Schaltkreise (Mikrochips) können in Substrate eingearbeitet werden. Diese dienen zum Speichern und Verarbeiten von Daten in digitalisierter Form. Das Auslesen erfolgt über elektrischen Kontakt mittels der sichtbaren Teile des Chipmoduls.

Beispiel: Geldkarte

Quellen: Gie-13a, Rat-13

Abbildung A-8: Mikrochip mit Kontakt [Rat-13]

A.3.6 Radiofrequenzidentifikation (RFID)

Detektion von und Datenaustausch mit Transpondern über ein (elektro-) magnetisches Feld bestimmter Frequenzen (siehe auch Abschnitt 7.4, S. 160).

Beispiel: Behälteridentifikation, Objektidentifikation

Quellen: Abe-11, Abr-10, Bun-05, Fuc-06, Gau-12, Gie-13a, Gün-11a, Hop-03, ICC-06, Krü-04, Krü-06, Pro-12, Rat-13, Sil-08, Sit-06, Sok-06, Sta-07, Sta-08, Ste-11a, Wil-07, Win-07

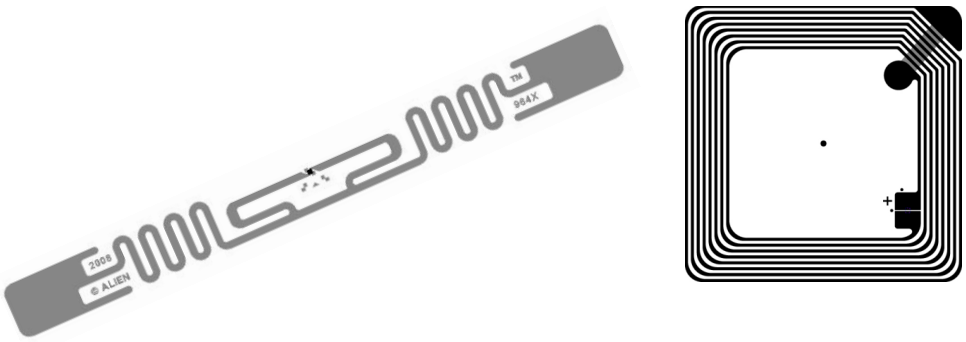


Abbildung A-9: UHF-Transponder (links) und HF-Transponder, [Ali-13a] und [Ave-13]

A.4 Haptische Sicherheitsmerkmale

A.4.1 Druckverfahren

A.4.1.1 Hochdruck

Druckverfahren, bei dem die druckenden Teile erhaben sind. Charakteristische Merkmale sind Prägespuren auf dem Bedruckstoff und ein vom eigentlichen Zeichen leicht abgesetzter Quetschrand, also ein Farbrand rund um den Abdruck.

Beispiel: Sicherheitsdokumente

Quellen: Rat-13

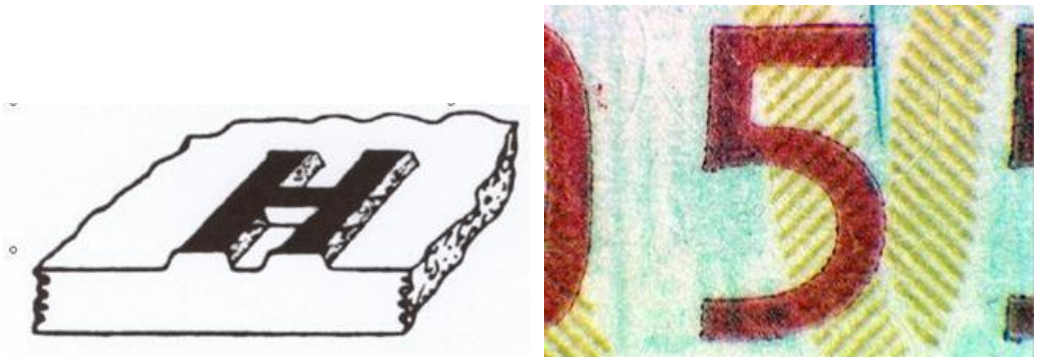


Abbildung A-10: Hochdruckform für Buchstaben (links) und gedruckte Ziffer [Rat-13]

A.4.1.2 Matrixdruck / Nadeldruck

Bei diesem Impact-Druckverfahren wird die Bildinformationen unter Verwendung eines Farbbandes und einer Punktmatrix, mit der unterschiedliche Zeichen bzw. Zeichensätze erzeugt werden können, auf das Substrat übertragen.

Beispiel: Ausweise

Quellen: Rat-13

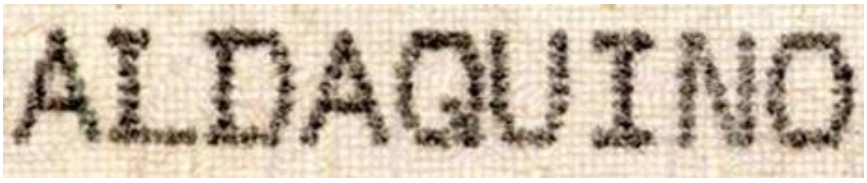


Abbildung A-11: Nadeldruck [Rat-13]

A.4.1.3 Tiefdruck

Beim Tiefdruck werden die drei folgenden Verfahren unterschieden.

A.4.1.3.1 Intagliodruck / Stichtiefdruck

Beim Stichtiefdruck werden Druckformen durch Ätzen oder Gravieren erzeugt. Die tiefer liegenden Bereiche tragen dickflüssige und hochpigmentierte Druckfarbe, die unter hohem Druck (mehreren Tonnen pro cm^2) auf das Substrat übertragen wird. Dabei wird das Substrat in die tiefer liegenden Teile der Druckplatte gepresst, wodurch ein erhabenes Abbild entsteht, das fühlbar und in Streiflicht sichtbar ist.

Beispiel: Ausweise, Banknoten

Quellen: Bun-05, Fuc-06, Gau-12, Gie-13a, Gün-11a, Hop-03, ICC-06, Rat-13, Wel-07

Abbildung A-12: Fühlbarer Stichtiefdruck [Rat-13]

A.4.1.3.2 Orlof-Technik / Schabloneneinfärbetechnik

Bei der Orlof-Technik handelt es sich um eine Einfärbetechnik beim Stichtiefdruck, um mit einer Druckform mehrere Farben gleichzeitig und präzise drucken zu können. Dabei werden die Einzelfarben so aufgebracht, dass die gewünschten Bereiche entsprechend eingefärbt sind. Die Farben können geringfügig überlappen. Daher ist auf dem fertigen Druckbild ein minimaler Farbübergang festzustellen.

Beispiel: Ausweise

Quellen: Rat-13

Abbildung A-13: Orlof-Technik / Schabloneneinfärbetechnik [Rat-13]

A.4.1.3.3 Rastertiefdruck

Druckformen mit tiefer liegenden Bereichen (Tiefdrucknäpfchen), in denen die Druckfarbe für den Druck enthalten ist, erzeugen das Druckbild. Die Menge des Farbauftrags hängt von Tiefe und Größe der Tiefdrucknäpfchen ab, die Näpfchenstruktur ist im Druckbild erkennbar.

Beispiel: Ausweise

Quellen: Rat-13

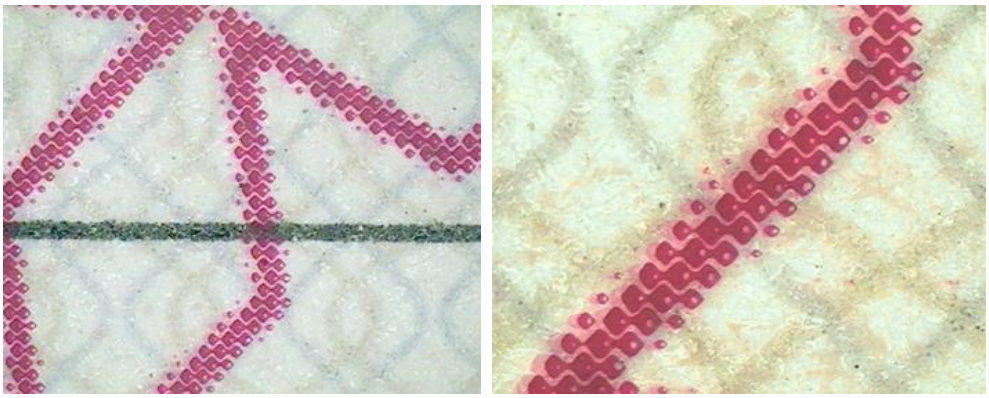


Abbildung A-14: Rastertiefdruck [Rat-13]

A.4.1.4 Siebdruck

Beim Siebdruck wird Farbe durch die durchlässigen Bereiche eines Siebs (Maschen) auf das darunter befindliche Substrat zum Auftrag dickerer Farbschichten gepresst. Es entsteht eine sägezahnartige Siebstruktur an den Rändern, der Druck ist erhaben und fühlbar.

Beispiel: Ausweise, Aufbringen von Effektfarben wie irisierende Farbe

Quellen: Gau-12, Gie-13a, Gün-11a, Rat-13

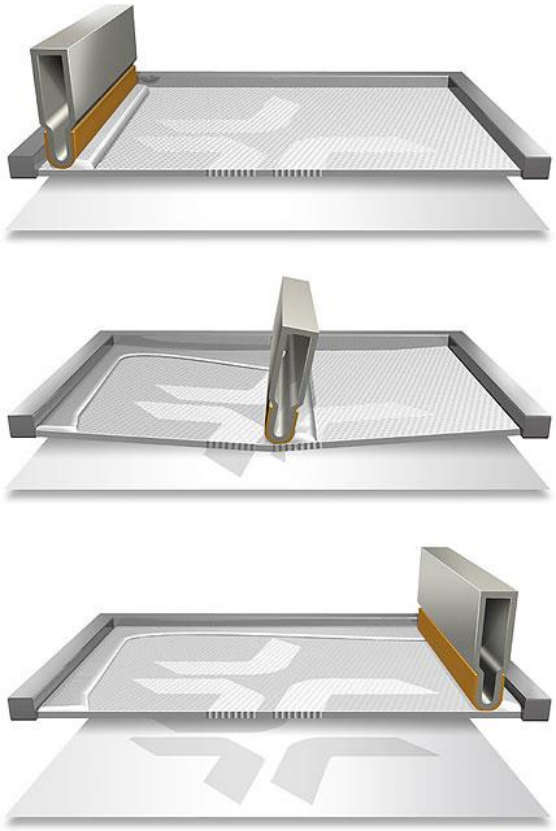


Abbildung A-15: Siebdruck [Dru-13]

A.4.2 Prägen

A.4.2.1 Blindprägung

Unter Blindprägen versteht man die Erzeugung eines fühlbaren Motivs – erhaben oder vertieft – ohne zusätzliche Farbe unter hohem Druck und bei bestimmten Temperaturen. Abhängig des Substrats können verschiedene Prägeverfahren zur Anwendung kommen:

- Prägestempelabdruck
- Folienprägung
- Blindpressen / Reliefprägung

Beispiel: Sicherheitsdokumente, PEAK®

Quellen: Aus-13a, Aus-13b, Bun-05, Bun-12a, Gau-12, Gie-13a, Gün-11a, Hoc-13, Krü-06, Mal-05, Rat-13, Sok-06, Wel-07

Abbildung A-16: Reliefprägung [Rat-13]

A.4.2.2 Heißfolienprägung

Übertragung von Schichten einer Prägefolie mithilfe eines Prägestempels unter der Wirkung von Druck und Temperatur auf das Substrat – die Temperaturen sind folien- und substratabhängig bei beispielsweise 80°C bis 220°C. Die optisch wirksame Schicht kann Farbpigmente, Metallpigmente oder Lacke enthalten und zu sehr unterschiedlichen visuellen Effekten führen.

Beispiel: Ausweise

Quellen: Hoc-13, Rat-13

Abbildung A-17: Heißfolienprägung [Rat-13]

A.5 Optische Sicherheitsmerkmale

A.5.1 Optische Effekte

A.5.1.1 Durchsichtsfenster

Bei Durchsichtsfenstern gibt es zwei verschiedene Arten.

A.5.1.1.1 Foliendurchsichtsfenster

In Dokumente, bei denen als Substrat Polymer verwendet wird, können Durchsichtfenster eingearbeitet werden, die vor hellem Hintergrund ein anderes Motiv zeigen als vor einem dunklen Hintergrund.

Beispiel: Banknoten, varifeye®

Quellen: Fuc-06, Gie-13a

Abbildung A-18: Foliendurchsichtsfenster in einer Musterbanknote (oben), das vor hellem Untergrund (unten links) anders erscheint, als vor dunklem Hintergrund (unten rechts) [Gie-13b]

A.5.1.1.2 Moiré Magnifier-Element

Durchsichtsfenster mit mikrooptischen Linsen, die Mikrostrukturen vergrößern und beim Kippen einen Motivwechsel von völlig unterschiedlichen, dreidimensionalen Motiven erscheinen lassen.

Beispiel: Banknoten; varifeye® Magic™

Quellen: Aus-13b, Gie-13a, Lou-13

Abbildung A-19: Moiré Magnifier-Element [Gie-13a]

A.5.1.2 Durchsichtsregister

Das Durchsichtsregister ist ein sich ergänzendes, auf Vorder- und Rückseite eines durchscheinenden Papiers aufgeteiltes Muster.

Beispiel: Banknoten

Quellen: Aus-13a, Bun-12a, Fuc-06, Gie-13a, Hop-03, Mal-05, Rat-13

Abbildung A-20: Durchsichtsregister [Deu-13a]

A.5.1.3 Hologramme

Hologramme zeigen abhängig des Beleuchtungs- und Betrachtungswinkels unterschiedliche Muster, Farben und Motive. Es existieren viele unterschiedliche Varianten und verschiedene Sicherheitsgrade. Dabei werden beispielsweise unterschieden das Hologramm, das 2D-Hologramm, das 2D- / 3D-Hologramm und das 3D-Hologramm. Auch unsichtbare Merkmale können eingebracht werden, die nur mit Spezialgeräten lesbar sind. Zusätzlich gibt es die unterschiedlichen Ausprägungen:

- Computergenerierte Hologramme (CGH):
  synthetische, mithilfe des Computers erzeugte Hologramme
- Hologramme mit Informationen:
  Abbildung von Informationen in Hologrammen, die versteckt und für das menschliche Auge nicht sichtbar sind, Prüfung mittels bestimmter optischer Linsen

- Kinegramme / Multiplexhologramme:
  Darstellung filmähnlicher Bewegungen, Herstellung sehr aufwendig
- Prägehologramme:
  Herstellung kompliziert und sehr aufwändig, aber in großen Stückzahlen wirtschaftlich – daher sind Prägehologramme die am meisten verwendeten Hologramme
- Transmissionshologramme:
  Hologramme, bei denen zur Aufnahme und Rekonstruktion Laserlicht benötigt wird
- Weißlichthologramme:
  Hologramme, die erst bei Beleuchtung mittels normalem, weißem Licht in einem vorgeschriebenem Winkel erscheinen

Beispiel: Banknoten, Kreditkarten, Handyakkus; intraGRAM®, Kinegram®, Identigram®, Exelgram®, Movigram®, Pixelgram®, Stereogram®

Quellen: Abe-11, Aus-13a, Aus-13b, Bun-05, Bun-12a, Fuc-06, Gau-12, Gie-13a, Hop-03, ICC-06, Kok-02, Krü-04, Krü-06, Mei-11, Mal-05, Möh-12, Pro-12, Rat-13, Sit-06, Sok-06, Ste-11a, Völ-13, Wel-07, Wil-07, Win-07

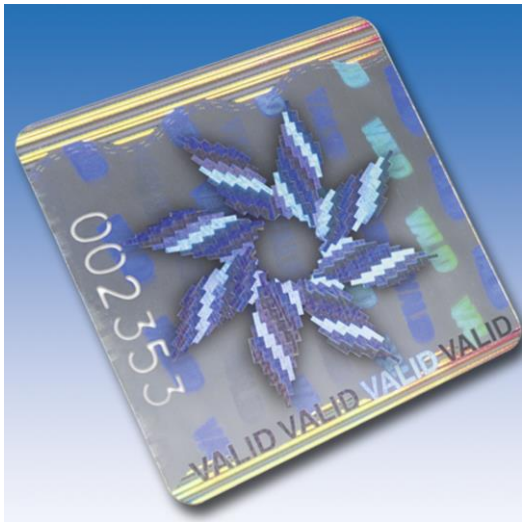


Abbildung A-21: Hologramm [Sch-13a]

A.5.1.4 Laserkippbild

Unter den, aus verschiedenen Winkeln belaserten, zylindrischen Linsen erscheint je nach Blickwinkel ein völlig anderes Motiv wie beispielsweise ein Foto, ein Logo oder auch Daten.

Beispiel: Changeable Laser Image (CLI®), Multiple Laser Image (MLI®)

Quellen: Aus-13a, Aus-13b, Bun-05, Bun-12a

Abbildung A-22: Laserkippbild [Aus-13a]

A.5.1.5 Parallaxe

Sicherheitsmerkmal, bei dem eine scheinbare Veränderung der Position eines Objektes bei Veränderung des Betrachtungswinkels stattfindet.

Beispiel: 3M™ Floating Image

Quellen: [3M-13]

Abbildung A-23: Der Parallaxeneffekt bewirkt bei diesem Muster, dass das rote Logo und die blaue Fahne sich bei unterschiedlichen Betrachtungswinkeln gegeneinander verschieben [3M-13]

A.5.1.6 Retroreflektierende Folie

Die retroreflektierende Folie kann ein verborgenes Motiv integrieren, das bei Beleuchtung mit Koaxiallicht und der Verwendung einer speziellen Optik sichtbar wird.

Beispiel: Ausweise

Quellen: Rat-13

Abbildung A-24: Reisepass der Niederlande unter Normallicht (links) und Koaxiallicht [Rat-13]

A.5.1.7 Wasserzeichen

Ein Wasserzeichen ist ein, aufgrund unterschiedlicher Papierstärken im Papier, durchscheinendes Hintergrundbild. Dabei gibt es verschiedene Ausprägungen:

- Langsiebwasserzeichen
- Rundsiebwasserzeichen
- Elektrotype

Beispiel: Banknoten

Quellen: Bun-05, Fuc-06, Gie-13a, Hop-03, ICC-06, Krü-06, Mal-05, Rat-13, Sok-06, Wel-07

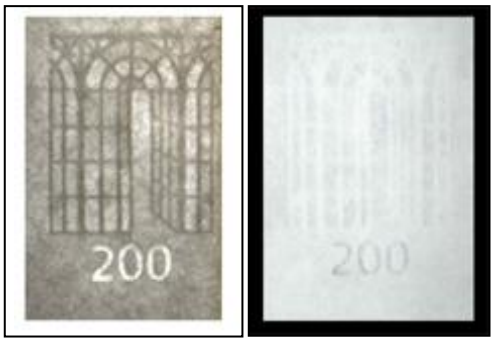


Abbildung A-25: Wasserzeichen der 200-Euro-Banknote im Gegenlicht (links) und auf dunklem Untergrund [Deu-13a]

A.5.2 Pre-Press-Druckmerkmale

Pre-Press-Druckmerkmale sind Merkmale, die vor dem Druck in der sogenannten Druckvorstufe in das Druckbild eingebracht werden und nach dem Druck sichtbar oder für Menschen unsichtbar vorhanden sind. Dabei gibt es verschiedene Möglichkeiten, die im Folgenden dargestellt werden.

A.5.2.1 Anti-Kopier-Muster

Anti-Kopier-Muster können versteckte Informationen im Untergrunddruck sein, die beim Kopieren sogenannte Interferenzmuster hervorrufen und eine eindeutige Unterscheidbarkeit vom Original zur Folge haben. Auch kann ein feines Linienraster verwendet werden, dessen Linien bei einem Kopierversuch zulaufen und so zu störenden Bildelementen führen.

Beispiel: Ausweise

Quellen: Bun-05, Bun-12a, Rat-13, Völ-13

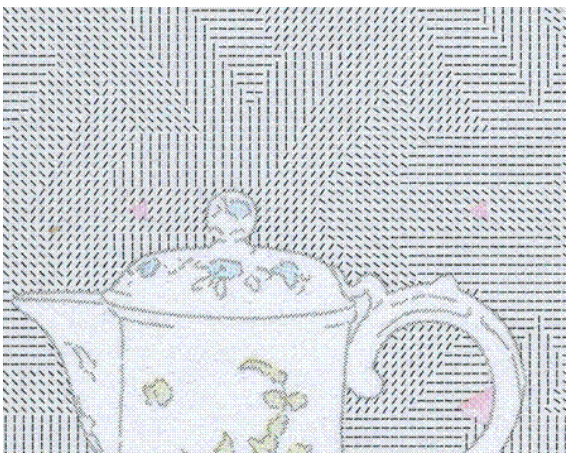


Abbildung A-26: Kopierschutzmuster im Reisepass der Niederlande als feine winkelabhängige Strichstrukturen [Rat-13]

A.5.2.2 Besondere Schriftart

Verwendung einer Schriftart, die keine der Standard-Schriftarten oder Standard-Drucktypen ist.

Beispiel: Dokumente der Technischen Universität München werden mit einer speziellen Hausschrift gedruckt [TUM-13]. Diese wurde auch für die vorliegende Arbeit verwendet.

Quellen: Rat-13

A.5.2.3 Digitale Wasserzeichen

Durch Veränderung der Druckdaten eines Druckbildes können digitale Wasserzeichen erzeugt werden. Dabei kommen kryptografische und steganografische Techniken in der Druckvorstufe zum Einsatz. Ergebnis sind kaum sichtbare, aber maschinenlesbare Informationen, die anschließend im Druckbild vorhanden sind. Es sind auch binäre Daten im digitalen Wasserzeichen abbildbar.

Als bekanntes Beispiel kann hier die Farbdruckermarkierung Machine Identification Code (MIC) angeführt werden, die auch die Bezeichnungen yellow dots, tracking dots oder secret dots trägt. Diese Markierung wird von bestimmten Farbdruckern und -kopierern auf jeder Seite mitgedruckt und ermöglicht eine Identifikation des Geräts, auf dem ein bestimmtes Schriftstück erzeugt wurde.

Beispiel: Machine Identification Code (MIC), scryptoPRINTTM, Cryptoglyph

Quellen: Alp-13, Fuc-06, Gau-12, Gün-11a, Hop-03, ICC-06, Krü-06, Mal-05, Pro-12, Sok-06, Ste-08, Völ-13, Wel-07, Wil-07

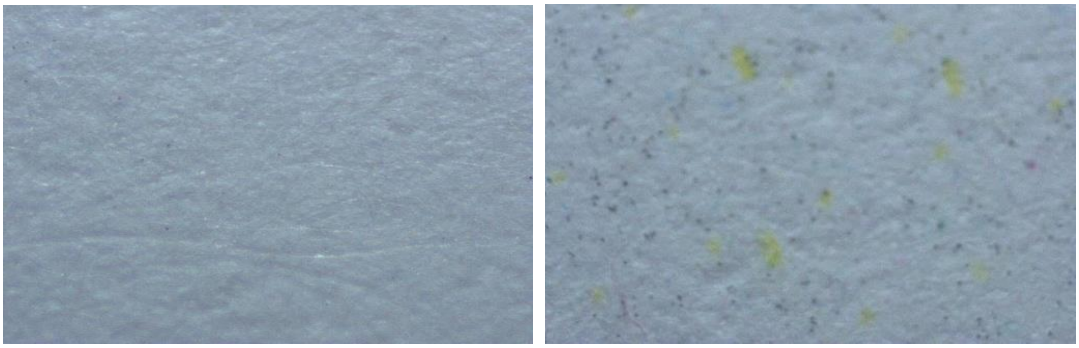


Abbildung A-27: Unbedruckte Seite (links) und bedruckte Seite eines Farb-Laser-Druckers mit Machine Identification Code [Ele-13]

A.5.2.4 Mikrotext

Mikrotext existiert in drei Ausführungen:

- Minischrift mit einer Schrifthöhe kleiner 0,8mm
- Mikroschrift mit Schrifthöhen kleiner 0,3mm
- Nanoschrift mit Schrifthöhen kleiner 0,2mm

Beispiel: Banknoten

Quellen: Aus-13a, Aus-13b, Bun-05, Bun-12a, Gau-12, Gün-11a, ICC-06, Krü-04, Krü-06, Mei-11, Rat-13, Sil-08, Sit-06, Völ-13, Wel-07

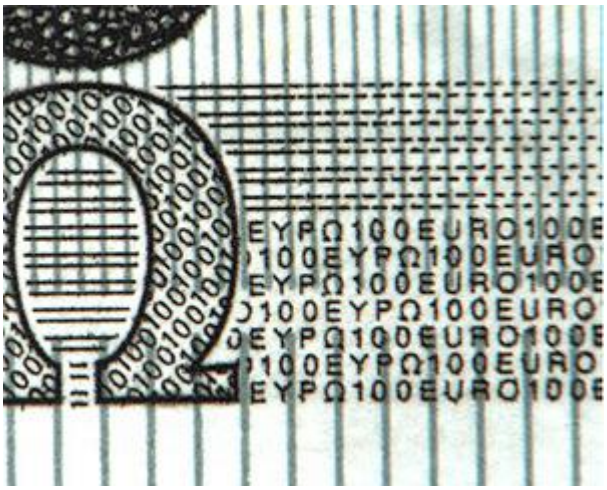


Abbildung A-28: Mikrotext einer 100-Euro-Banknote [Deu-13a]

A.5.2.5 Rasterbild

Unsichtbare Informationen im Druckraster, die mit Spezialfolien unter Ausnutzung des Moiré-Effektes sichtbar gemacht werden können. Dabei sind Bilddarstellungen oder Text möglich.

Beispiel: Verpackungen

Quellen: Aus-13a, Mei-11

Abbildung A-29: Rasterbild (links) wird durch den Spezialfilter zu einem Prüfmuster [Aus-13a]

A.5.2.6 Scrambled image / codiertes Bild

Ein Scrambled Image ist eine Information im Untergrunddruck. Das Bild ist nur mittels einer Decodierlinse oder Laborgeräten (Scanner und Rechner mit spezieller Bildbearbeitungssoftware) erkennbar.

Beispiel: Ausweise

Quellen: Rat-13

A.5.3 Spezialdruck

A.5.3.1 Guillochen

Guillochen sind spezielle Muster oder Ornamente aus mehreren ineinander verschlungenen und überlappenden Linienzügen. Die einzelnen Linien sind als schnurartige, oft asymmetrische, geschlossene Ellipsen oder auch Kreisbahnen ausgeprägt. Hergestellt werden diese mit kostenintensiven Guillochiermaschinen.

Beispiel: Ausweise, Banknoten

Quellen: Aus-13a, Aus-13b, Bun-05, Bun-12a, Fuc-06, Gau-12, Gün-11a, ICC-06, Krü-04, Krü-06, Mei-11, Rat-13, Sit-06, Sok-06, Völ-13, Wel-07

Abbildung A-30: Positiv- und Negativguillochen im Reisepass der Tschechischen Republik [Rat-13]

A.5.3.2 Irisdruck / Regenbogendruck

Der sanfte Übergang von einer Farbe zur anderen und somit eine vermischte, ineinander laufende Wiedergabe wird als Irisdruck bezeichnet.

Beispiel: Sicherheitspapiere

Quellen: Aus-13a, Aus-13b, Bun-05, Bun-12a, Fuc-06, Krü-06, Rat-13, Sok-06, Wel-07

Abbildung A-31: Irisdruck [Rat-13]

A.5.4 Spezialfarben / Spezialpartikel

A.5.4.1 Clustermerkmal

Das Clustermerkmal ist ein spezieller Farbeffekt der Clusterschicht, die durch Elektronenstrahlbedampfung oder mithilfe des Sputter-Verfahrens hergestellt wird. Dabei erzeugen mehrere Schichten aufgrund ihrer filternden bzw. diffraktiven Eigenschaften einen Farbumschlag. Das abgebildete Farbspektrum enthält zwei Maxima (z. B. magenta und grün oder blau und grün), die mittels der verwendeten Materialien und Schichtdicken präzise eingestellt und mit Handlesegeräten erfasst und ausgewertet werden können.

Beispiel: Colour-Switch-Folie, ClusterSecure

Quellen: Abe-11, Gau-12, Gün-11a, Mal-05, Mue-13, Ste-11a, Win-07

Abbildung A-32: Clustermerkmal [Gün-11a]

A.5.4.2 Fotochrome Farbe

Fotochrome Farbe ist eine Farbe, die sich unter Lichteinwirkung verändert. Dieser Farbumschlag kann reversibel oder irreversibel sein.

A.5.4.2.1 Reversible fotochrome Farbe

Einfallendes Licht erzeugt einen vorübergehenden Farbumschlag, der sich bei Wegfall der Lichtquelle wieder umkehrt, die Farbe erscheint wieder wie im Ausgangszustand.

Beispiel: kurzzeitige, schlagartige Farbveränderung durch Lichteinfall beim Fotokopieren, die eine Reproduktion auf diesem Weg verhindert

Quellen: Fuc-06, Gau-12, Gün-11a, ICC-06, Kok-02, Krü-06, Rat-13

Abbildung A-33: Farbwechsel von photochromer Farbe unter UV-Licht [Rat-13]

A.5.4.2.2 Irreversible fotochrome Farbe

Einfallendes Licht erzeugt einen Farbumschlag, der dauerhaft vorhanden bleibt.

Beispiel: permanent vorhandener Farbumschlag bei Auftreffen von ultraviolettem (Tages-)Licht

Quellen: Gün-11a, ICC-06

A.5.4.3 Fluoreszenz

Bei Fluoreszenz regt Energiezufuhr Substanzen kurzzeitig zum Leuchten an. Anders als bei der Phosphoreszenz hält das Leuchten zwischen etwa 10^{-10}s bis 10^{-7}s nach der Anregung an – diese Zeitdauer wird auch als Abklingzeit bezeichnet. Die Anregung kann unterschiedlich erfolgen: Einstrahlung von Licht, Bestrahlung mit Röntgenstrahlen, Beschuss mit Elektronenstrahlen, radioaktive Bestrahlung, elektrische Felder, chemische Reaktionen, mechanische Beanspruchung, thermische Einwirkung. Die absorbierte Energie wird in Form von elektromagnetischer Strahlung gleicher oder längerer Wellenlänge wieder abgeben. In den folgenden Unterabschnitten werden verschiedene Sicherheitsmerkmale, die mit Fluoreszenz arbeiten, vorgestellt.

Beispiel: Fluorit, Uranylsalze, Salze der Seltenerdmetalle, Anthracen, Naphthalin, Stilben; Tailor-Safe®

Quellen: Ble-13, Bro-13a

A.5.4.3.1 Infrarotfarbe

Infrarotfarbe (IR) ist eine Farbe, die Infrarotstrahlung absorbiert oder bei Anregung mit Infrarotlicht entweder Infrarotlicht oder sichtbares Licht zurück strahlt. Dabei sind unternehmens- oder produktindividuelle Spektren darstellbar.

Beispiel: Infrarot-Testkarte mit Farbfeld zum Test von Infrarot-Fernbedienungen, Lasersecure®

Quellen: Abe-11, Aus-13a, Aus-13b, Bun-05, Fuc-06, Gie-13a, Gün-11a, Hop-03, ICC-06, Kok-02, Krü-06, Mal-05, Mei-11, Pro-12, Rat-13, Sil-08, Völ-13, Wel-07

Abbildung A-34: Infrarotfarbe ohne (links) und mit Infrarotlichtbestrahlung [Aus-13a]

A.5.4.3.2 Röntgenlumineszenz

Die Anregung bestimmter chemischer Substanzen mit Röntgenstrahlen veranlasst diese zu einem charakteristischen Leuchten. Bei Verwendung als Sicherheitsmerkmal werden Partikel im Nanometerbereich dem Grundsubstrat eines Produkts beigemischt und sind temperaturbeständig bis über 1.700 °C. Die Feststellung der Stoffeigenschaften, also der Zusammensetzung, und der Stoffmengen, also der Konzentration, ermöglicht eine Authentifizierung mit Röntgenfluoreszenz-Spektrometern.

Beispiel: Lanthanoide, Yttrium, Zink, Molybdän; Polysecure, Traceless

Quellen: Fuc-06, Gau-12, Gün-11a, Pol-13

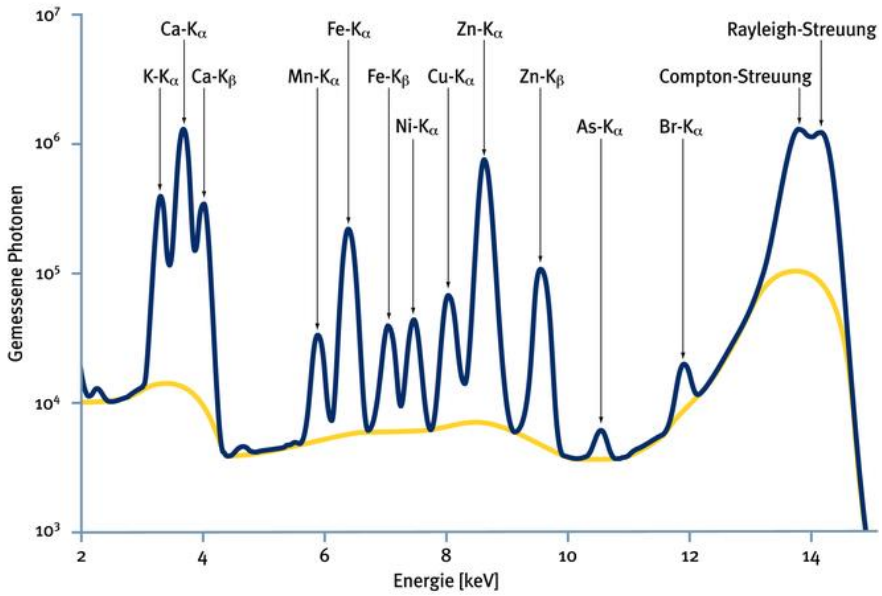


Abbildung A-35: Röntgenfluoreszenzspektrum einer Probe mit Benennung der wichtigsten sichtbaren Signale über dem gelben Untergrund [Deu-13b]

A.5.4.3.3 Tagesleuchtfarbe / Neonfarbe als Echtfarbelement

Tagesleuchtfarben sind Farben mit Farbpartikeln mit hoher Leuchtkraft. Diese entsteht aufgrund der Umwandlung des blauen Lichtanteils und des Lichts nahe dem ultravialetten Lichtbereich in Licht größerer Wellenlänge. Diese Farben sind mit handelsüblichen (Farb-)Kopierern nicht kopierbar, da die Farben außerhalb der gebräuchlichen Cyan-Magenta-Gelb-Schwarz-Farbpalette (cmyk-Farbpalette) bzw. des häufig genutzten Rot-Grün-Blau-Farbraums (rbg-Farbraum) liegen.

Beispiel: Neon-Orange auf Fahrkarten

Quellen: Abe-11, Fuc-06, Gün-11a, Kok-02, Krü-06

Abbildung A-36: Tagesleuchtfarben auf Fahrscheinen [Dia-13]

A.5.4.3.4 Ultraviolette Farbe

Ultraviolette Farbe (UV) strahlt bei Anregung mit ultraviolettem Licht entweder ultraviolettes Licht oder sichtbares Licht (alle sichtbaren Farben von violett bis rot) zu-

rück. Kleinste Partikel können auch in Substrate eingebracht werden. Typisch sind hier die bekannten Melierfasern oder Planchetten.

Beispiel: Melierfasern in Banknoten, fluoreszierender Sicherheitsfaden, fluoreszierender Heftfaden, fluoreszierende Planchetten, Regenbogenfluoreszenz

Quellen: Abe-11, Aus-13a, Aus-13b, Bun-05, Bun-12a, Fuc-06, Gie-13a, Gün-11a, Hop-03, ICC-06, Krü-04, Krü-06, Mal-05, Mei-11, Rat-13, Völ-13, Wel-07

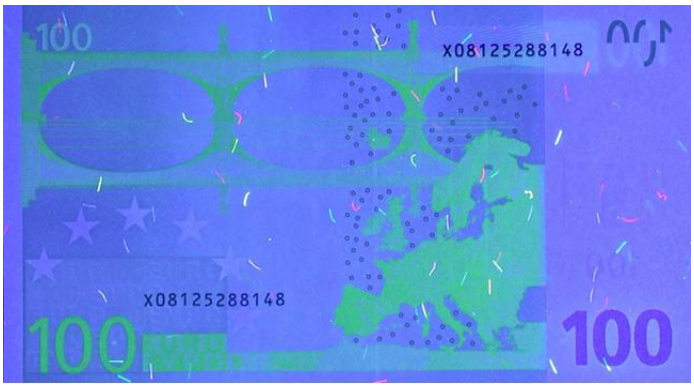


Abbildung A-37: Ultraviolette Farbelemente auf der 100-Euro-Banknote [Deu-13a]

A.5.4.4. Interferenz- und Effektfarbe

Bei dieser Farbe wird der physikalische Effekt der Interferenz ausgenutzt, der eine vom Betrachtungswinkel abhängige Coloristik erscheinen lässt. Dabei wird Licht zwischen dünnen, transparenten Schichten gebrochen und es entsteht eine irisierende Perlglanzerscheinung ähnlich wie bei Perlen, Muscheln oder Seifenblasen. Der Effekt kann auch mit Perlglanzpigmenten (auch Glimmerplättchen genannt) erzeugt werden. Dabei kommen plättchenförmige, transparente und nicht-transparente Pigmente der Größe 60µm bis 100µm zum Einsatz.

Beispiel: Iriodin, Meartite, Paliosecure, Paliochrom

Quellen: Bun-12a, Gie-13a, Hup-07, Hup-08, Kok-02, Krü-06, Pfa-07, Rat-13

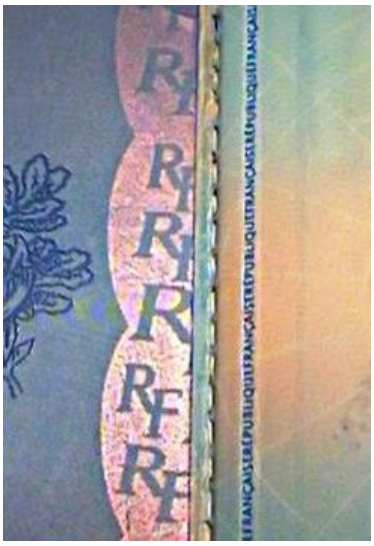


Abbildung A-38: Interferenzfarbe auf dem französischen Reisepass [Rat-13]

A.5.4.5 Kippfarbe / optisch variable Druckfarbe

Nur für Sicherheitsdruckereien zugängliche Sonderfarben mit einer, vom Betrachtungswinkel abhängigen farblich unterschiedlichen Erscheinung. Spezielle, kundenindividuelle Farbkombinationen sind realisierbar: beispielsweise verändert sich violett unter anderem Betrachtungswinkel ins grün-bräunliche. Das Auslesen über spezielle Filter oder Lesegeräte ist möglich.

Beispiel: Banknoten

Quellen: Abe-11, Aus-13a, Aus-13b, Bun-05, Abe-11, Bun-12a, Fuc-06, Gie-13a, Gün-11a, Hop-03, Krü-04, Krü-06, Mal-05, Mei-11, Pro-12, Rat-13, Sit-06, Sok-06, Völ-13

Abbildung A-39: Kippfarbe aus verschiedenen Betrachtungswinkeln – als Prüfelement auf einem Muster (links) oder in Anwendung auf der 50-Euro-Banknote, [Sch-13a] und [Deu-13a]

A.5.4.6. Magnetisierbare Farbe

Nach Auftrag der Farbe mit ferromagnetischen Spezialpartikeln wird diese mit einem Vibrations-Magnetometer behandelt. Durch die zufällige Anordnung der magnetischen Partikel entsteht ein individuelles magnetisches Muster, das eindeutig erkannt werden kann und Produkte individualisiert. Der Nachweis erfolgt sensorisch mittels Magnetflussgerät.

Beispiel: Banknoten; Coded Ink Identification (CIID), MagDot

Quellen: ICC-06, Kok-02, Sil-08, Sok-06, Wel-07

A.5.4.7. Metallreagenzfarbe

Schwarz-gräuliche Verfärbung der unsichtbaren Metallreagenzfarbe (auch: Coin-Reactive-Ink) bei Reibung mit einem Metall.

Beispiel: Medikamentenverpackung, Sicherheitsdokumente

Quellen: Krü-04, Mei-11, Sit-06, Wel-07

Abbildung A-40: Verfärbung einer Metallreagenzfarbe [Con-13]

A.5.4.8. Metamere Farbe

Chemisch unterschiedliche Farbpaare erscheinen unter einer gegebenen Lichtquelle kaum unterschiedlich. Unter einer anderen Lichtart oder bei Betrachtung durch einen Filter, in der Regel einem Rotfilter, erscheinen diese jedoch in einem markanten Farbkontrast.

Beispiel: Sicherheitsdokumente

Quellen: Rat-13

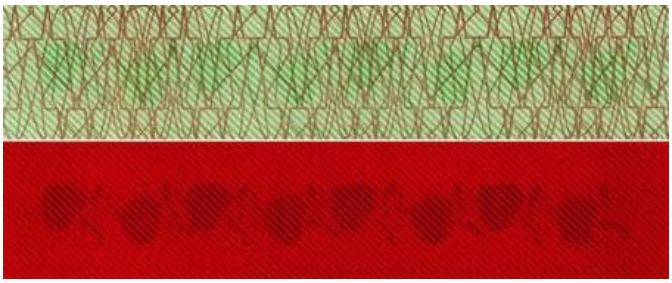


Abbildung A-41: Metamere Farbe [Rat-13]

A.5.4.9. Mikrofarbcode

Der Mikrofarbcode ist in Partikeln abgebildet, die aus mehreren Farbschichten aufgebaut sind. Dabei sind über 4,35 Millionen verschiedene Farbkombinationen möglich. Auch magnetische Schichten oder Schichten, die mit ultraviolettem oder Infrarotlicht anregbar sind, können integriert werden. Die Partikel haben eine Größe zwischen 5 µm und 75 µm – in manchen Quellen werden auch 1200 µm angeführt. Der individuelle Farbcode wird durch ein Mikroskop optisch geprüft.

Beispiel: Mikrotagganten®, Secutag®

Quellen: Abe-11, Fah-10, Fuc-06, Gau-12, Gün-11a, ICC-06, Kok-02, Kro-06, Krü-04, Mal-05, Mei-11, Pro-12, Sil-08, Sit-06, Ste-11a, Völ-13, Wel-07

Abbildung A-42: Mikrofarbcode als Animation (links) und Photographie, [3S-13] und [Mic-13]

A.5.4.10 Mikropunkte

Aufgesprühte Polyester-Mikropartikel mit einer Größe von 0,5 mm bis 1 mm mit aufgelasertem alphanumerischem Code können als Substratbeimischung im Produktionsprozess oder als Aerosolspray verwendet werden. Die Authentifizierung erfolgt mittels digitalem Speziallesegerät oder Mikroskop.

Beispiel: DataDotDNA, Mighty Dot, Securmark, Microdot

Quellen: Beh-13a, Dat-13b

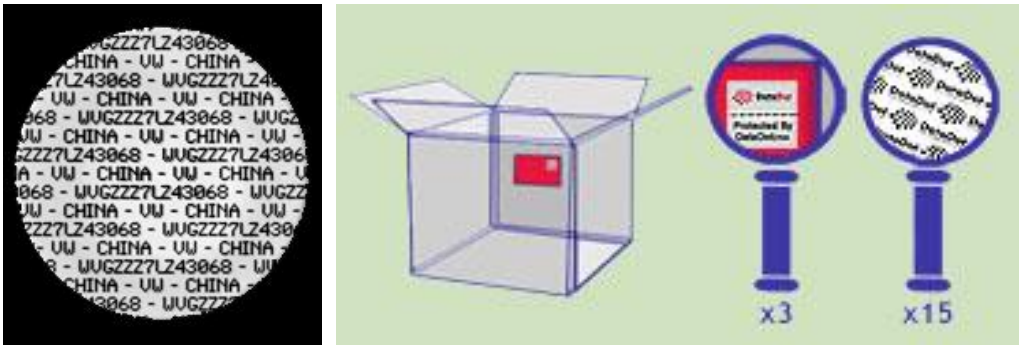


Abbildung A-43: Mikropunkte [Dat-13d]

A.5.4.11. Pen-Reactive-Ink / Reagenzfarbe

Farblose oder sichtbare Farbpigmente reagieren auf Testtinten mit einer Farbveränderung.

Beispiel: sichtbar machen transparenter Farbe durch Überstreichen mit einem Spezialstift

Quellen: Fuc-06, Kok-02

Abbildung A-44: Pen-Reactive-Ink [Shr-13]

A.5.4.12. Phosphoreszenz

Bei Phosphoreszenz regt Energiezufuhr Substanzen längerfristig zum Leuchten an: im Gegensatz zu Fluoreszenz mindestens 10^{-7}s, teilweise Sekunden, Minuten oder längeres Nachleuchten. Dabei kann Energie in verschiedenen Formen zugeführt werden: Einstrahlung von Licht, Bestrahlung mit Röntgenstrahlen, Beschuss mit Elektronenstrahlen, radioaktive Bestrahlung, elektrische Felder, chemische Reaktionen, mechanische Beanspruchung, thermische Einwirkung.

Beispiel: Seltene Erden, Zink-Sulfid-Kristalle; Tailor-Safe®

Quellen: Ble-13, Bro-13b, Ham-13, Krü-06, Tai-13

Abbildung A-45: Phosphoreszierende Farbpigmente [Tai-13]

A.5.4.13 Sicherheitsfärbemittel

Diese Färbemittel verfärben ein Dokument bei Manipulationsversuchen durch Lösungsmittel.

Beispiel: Sicherheitspapiere

Quellen: ICC-06, Mei-11

A.5.4.14 Sonderfarbe

Farben außerhalb der gebräuchlichen cmyk-Farbpalette bzw. des rbg-Farbraums verhindern Kopien mit handelsüblichen Kopierern.

Beispiel: Gold-, Silber-, Bronzedruckfarbe

Quellen: Abe-11, Gau-12, Gün-11a, Kok-02, Rat-13

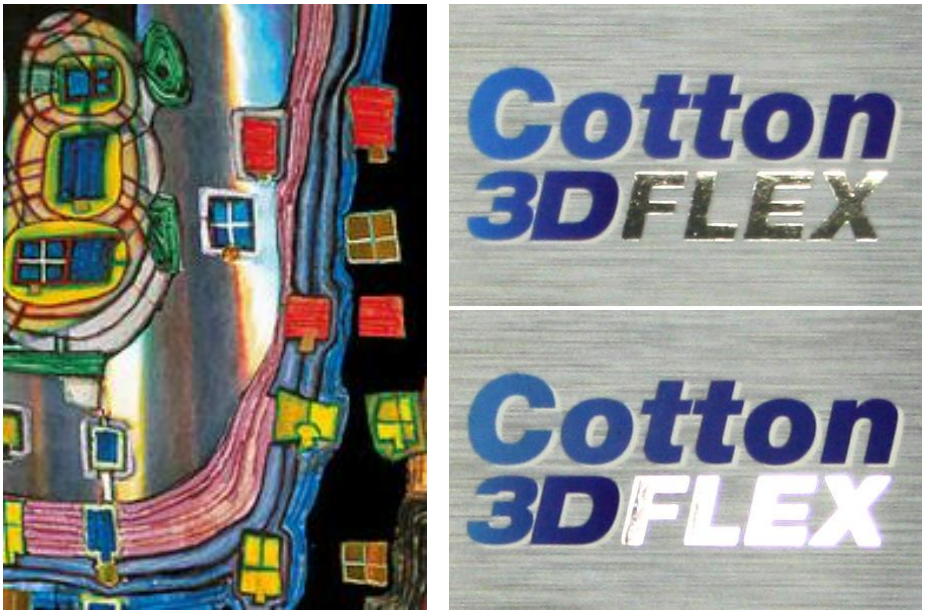


Abbildung A-46: Verwendung von Silberdruckfarbe auf einem Kunstdruck [Wör-13] und auf einer Verpackung eines Konsumguts

A.5.4.15 Spektralsensible Farbe

Die Farbe erscheint erst unter einer speziell farblich abgestimmten Beleuchtung.

Quellen: Sil-08

A.5.4.16 Thermoreaktive Farbe

Die thermoreaktive Farbe existiert in zwei Ausführungen, die in den beiden folgenden Abschnitten dargestellt werden.

A.5.4.16.1 Thermische Pigmente

Thermische Pigmente zeigen eine irreversible Farbveränderung bei Temperaturänderung.

Beispiel: Fresh Check, OnVu-Etikett, CheckPoint

Quellen: Gün-11a, ICC-06, Krü-04, Mei-11, Sil-08, Sit-06

A.5.4.16.2 Thermochrome Pigmente

Bei thermochromer Farbe ist die Farbveränderung, die bei einer Temperaturänderung eintritt, reversibel. Der Farbumschlag ist einstellbar auf verschiedenen Temperaturen. Auch die farbliche Reaktion ist unterschiedlich, beispielsweise werden farblose Pigmente bei Abkühlung farbig oder es zeigt sich ein Farbumschlag zwischen zwei Farben.

Quellen: Bun-12a, Fuc-06, Gie-13a, Gün-11a, Hop-03, ICC-06, Kok-02, Krü-04, Krü-06, Mal-05, Mei-11, Rat-13, Sil-08, Sit-06, Völ-13

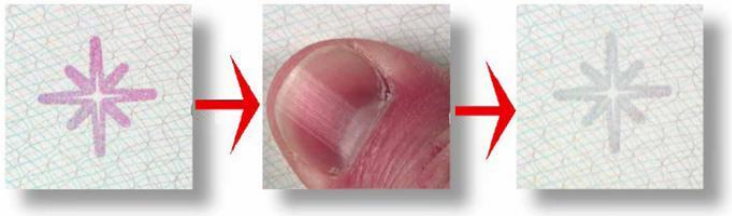


Abbildung A-47: Thermochrome Farbpigmente [Rat-13]

A.5.5 Sonstige

A.5.5.1 Feuchtstempelabdruck

Ein Feuchtstempelabdruck entsteht durch Auftragen flüssiger Druckfarbe mit einem Stempel.

Beispiel: (Sicherheits-) Dokumente

Quellen: Rat-13

Abbildung A-48: Feuchtstempelabdruck [Rat-13]

A.5.5.2 Lasergravur

Bei Veränderung der Oberfläche eines zu beschrifteten Materials mit Hilfe eines Lasers entsteht eine Lasergravur. Die Beschriftung wird zu einem Bestandteil der Oberfläche und ist wasser- und wischfest.

Quellen: Aus-13b, Bun-05, Krü-06, Rat-13, Sil-08

Abbildung A-49: Lasergravur im deutschen Führerschein [Rat-13]

A.5.5.3 Oberflächenauthentifizierung

Bei diesem Verfahren werden Objekte mit Hilfe von optischen Spezialaufnahmen der Oberflächen authentifiziert. Die notwendigen Bildaufnahmen werden hierfür in einer Datenbank abgelegt und bei der Prüfung abgeglichen. Dabei können die folgenden drei Möglichkeiten genutzt werden.

A.5.5.3.1 Musteroberfläche

Zum Zweck der Oberflächenauthentifizierung werden gezielte Veränderungen der Oberfläche eines Gegenstandes vor Erzeugung eines Abbilds vorgenommen.

Quellen: Fra-11, Wil-07

A.5.5.3.2 Sprengprägen

Sprengprägen wird genutzt zur Strukturierung von Metalloberflächen entsprechend einem Wunschmuster. Der Sprengvorgang selbst erzeugt einmalige Merkmale und ist nicht identisch wiederholbar.

Beispiel: Nutzung in Spritzgusswerkzeugen zur Übertragung des entstandenen einmaligen Musters in Spritzgussteile

Quellen: Bad-12, Fra-11, ICT-13

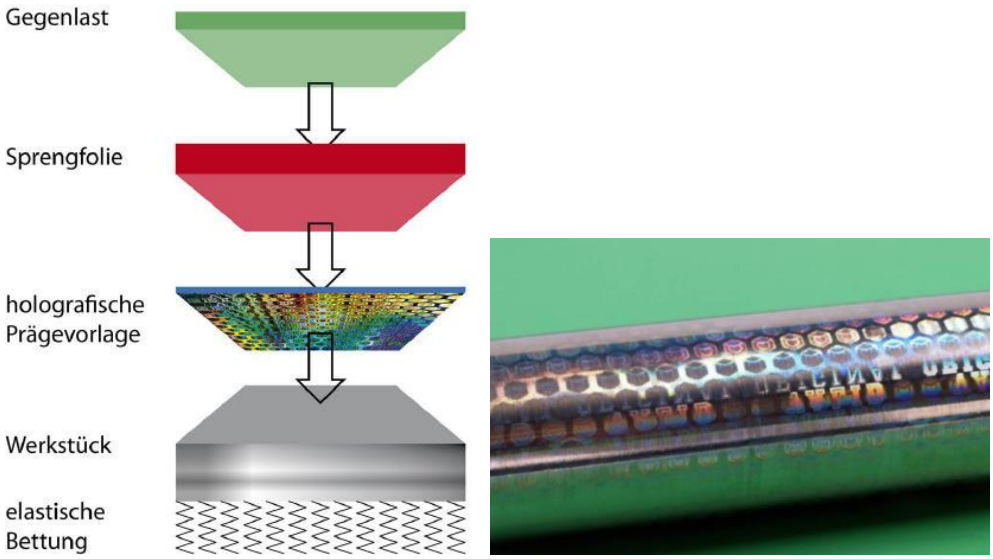


Abbildung A-50: Schematische Darstellung Sprengprägen (links) und erzieltes Ergebnis, [Fra-11] und [Bad-12]

A.5.5.3.3 Stochastische Schwankungen im Fertigungsprozess

Hier werden für eine Oberflächenauthentifizierung die Oberflächeneigenschaften ausgenutzt, die aufgrund stochastischer Schwankungen im Fertigungsprozess entstehen und nicht reproduzierbar sind. Das System zur Laseroberflächenauthentifizierung (LSA) ist ein typisches System dieser Gruppe und arbeitet bei der Authentifizierung mit einem Datenbankabgleich. Das Streulicht, das bei Abtastung einer bekannten Stelle eines Originalprodukts mit einer hoch fokussierten Lichtquelle entsteht, ist einzigartig (siehe Abbildung A-51). Das Ergebnis dieses Scans ist eine 10 Kilobyte große Datei und wird in einer Datenbank abgelegt. Bei der Authentifizierung wird das Ergebnis eines neuerlichen Scans mit den Daten in der Datenbank abgeglichen und die Originalität bestätigt oder widerlegt. [Brü-09, Gün-11a, Ste-11a, Uli-09]

Beispiel: Oberfläche eines Papiers, einer Holz- / Spanplatte, eines spanend bearbeiteten Produkts; Laseroberflächenauthentifizierung, scryptoTRACE®, SIGNOPTIC

Quellen: Abe-11, Brü-09, Gün-11a, Ste-11a, Uli-09

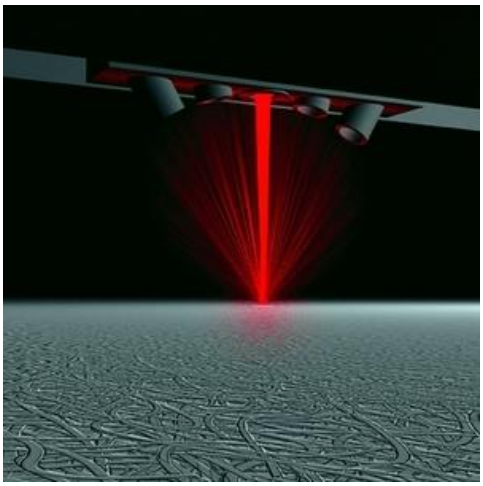


Abbildung A-51: Laseroberflächenauthentifizierung [Pro-13a]

A.5.5.4 Perforation

Eine Perforation kann auf zwei Wege erzeugt werden, die im Folgenden dargestellt sind.

A.5.5.4.1 Laserperforation

Mittels Laser können feinste Perforationen unterschiedlicher Art und Größe erzeugt werden.

Beispiel: Banknoten

Quellen: Bun-05, Bun-12a, Rat-13

Abbildung A-52: Perforation in Form des €-Zeichens im Hologramm der 50-Euro-Banknote [EZB-13b]

A.5.5.4.2 Nadelperforation

Bei der Nadelperforation wird mechanisch eine Lochung zur Darstellung von Zahlen oder Motiven mit fühlbaren Ausstichen (Graten) auf der Rückseite des Substrats er-

zeugt. Dabei entsteht eine gleichmäßige, matrixartige Formation von kreisrunden, gleich großen und immer aus der gleichen Richtung geführten Perforationslöchern.

Beispiel: Ausweise

Quellen: Rat-13

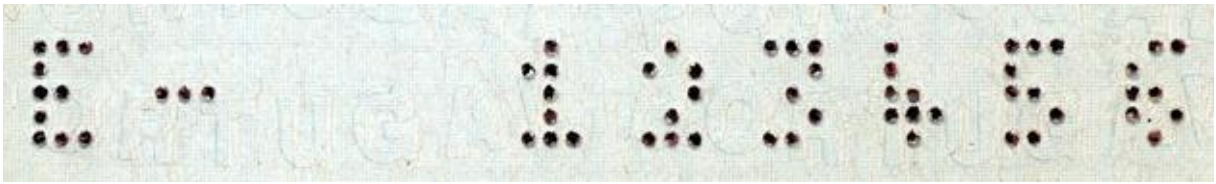


Abbildung A-53: Nadelperforation [Rat-13]

A.5.5.5 Rauschmustercodes

Rauschmustercodes sind sehr feine, im Rechner erzeugte, zufällige, digitale Muster, die auch Informationen codieren können. Aufgrund des prozessinhärenten Qualitätsverlusts beim Drucken können diese nicht exakt reproduziert werden (siehe Abbildung A-54). Die Authentifizierung erfolgt mittels spezieller, passend programmierter Lesegeräte im Offline-Modus, also ohne Datenbankabgleich.

Rauschmustercodes können auch als Unikatkennzeichen ausgeführt werden, kommen bislang aber meist als Originalitätskennzeichen zum Einsatz. Es handelt sich um gedruckte Schwarzweißmuster mit einer minimalen Größe von 12 mm^2, die aufgrund ihrer Auflösung nicht unerkannt kopiert werden können. Bei einer Authentifizierung wird der vorliegende Rauschmustercode optisch erfasst und gegen das passende digitale Profil geprüft. Dieses digitale Profil ist eine entsprechend abgeleitete und verschlüsselte Datei, aus der das Original-Rauschmuster nicht wieder hergestellt werden kann. [Ben-10, Vor-09, Web-07]

Die Authentifizierung kann online erfolgen, indem der Rauschmustercode beispielsweise mit einem Fotohandy oder Flachbettscanner erfasst und an einen Server gesendet wird. Dort wird das erfasste Bild auf Originalität überprüft und das Prüfergebnis mitgeteilt [Ben-10]. Für eine Offline-Authentifizierung muss das digitale Profil zuvor in einem 2D-Lesegerät abgelegt werden, das dann zur lokalen Authentifizierung verwendet werden kann (siehe Abbildung A-55). [Ben-10, Web-07]

Beispiel: BitSecure®, Copy Detection Pattern, Epicode

Quellen: Abe-11, Abr-10, Fah-10, Gün-11a, Krü-04, Mei-11, Pro-12

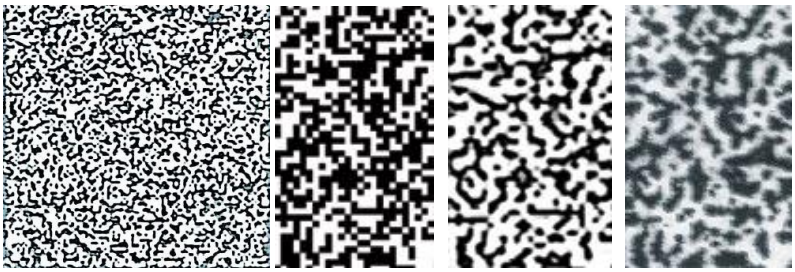


Abbildung A-54: Stark vergrößerter Rauschmustercode als Komplettdruck und in Ausschnitten als digitaler Version, als originaler Erstdruck und als Kopie (von links nach rechts), [Gün-11a] und [Ben-10]

Abbildung A-55: 2D-Lesegerät zur Authentifizierung eines Rauschmustercodes (links) sowie Authentifizierung mit einem Fotohandy, [Ben-10] und [Pro-13b]

A.5.5.6 Sicherheitsanstanzung

Eine Sicherheitsanstanzung entsteht durch bewusstes Stehenlassen von Material an einer Kontur. Dieser scheinbare Produktionsfehler kann für den Originalhersteller als Echtheitsmerkmal dienen.

Beispiel: Etiketten, Verpackungen

Quellen: Gün-11a

Abbildung A-56: Sicherheitsanstanzung [Gün-11a]

A.5.5.7 Sicherheitsfaden

Der Sicherheitsfaden ist ein meist metallisierter Folienstreifen mit einer Breite von 0,8 mm bis 5 mm, der in ein Substrat eingebracht wird. Dieser kann vollständig oder als Fensterfaden teilweise eingebettet sein. Zusätzliche Sicherheit entsteht durch Klartext- oder Farbelemente, Hologramm- oder Kippfarbenelemente, Magnetismus (sog. Magnetcode auf Euro-Banknoten), Fluoreszenz, Leitfähigkeit oder besondere Verarbeitung des Streifens.

Beispiel: Banknote

Quellen: Aus-13b, Bun-12a, Fuc-06, Gau-12, Gie-13a, Gün-11a, ICC-06, Krü-06, Rat-13, Wil-07

Abbildung A-57: Sicherheitsfaden 50-Euro-Banknote [Deu-13a]

A.6 Sonstige Sicherheitsmerkmale

A.6.1 Duftstoffe

Duftfarben oder Duftlacke mit speziellen, individuellen Duftmustern werden mit einem Handheld (Gaschromatograph) authentifiziert. Dabei wird das gemessene Duft-Muster mit gespeicherten Informationen in einer Datenbank abgeglichen.

Quellen: ICC-06, Sok-06

A.6.2 Markierung pulvermetallurgisch hergestellter Bauteile

Die eindeutige Identifikation von pulvermetallurgisch hergestellten Bauteilen (z. B. Sinterbauteile) ist mit Röntgenstrahlen oder Ultraschall möglich. Hierfür werden während des Herstellungsprozesses Fremdpartikel im Pulver platziert. Neben der Originalitätsaussage ist eine auslesbare binäre Information vorhanden. Diese ist aus der Anordnung der Fremdpartikel abzuleiten und mit deren Anzahl entsprechend begrenzt.

Quellen: Beh-07, Beh-13b, Ins-13

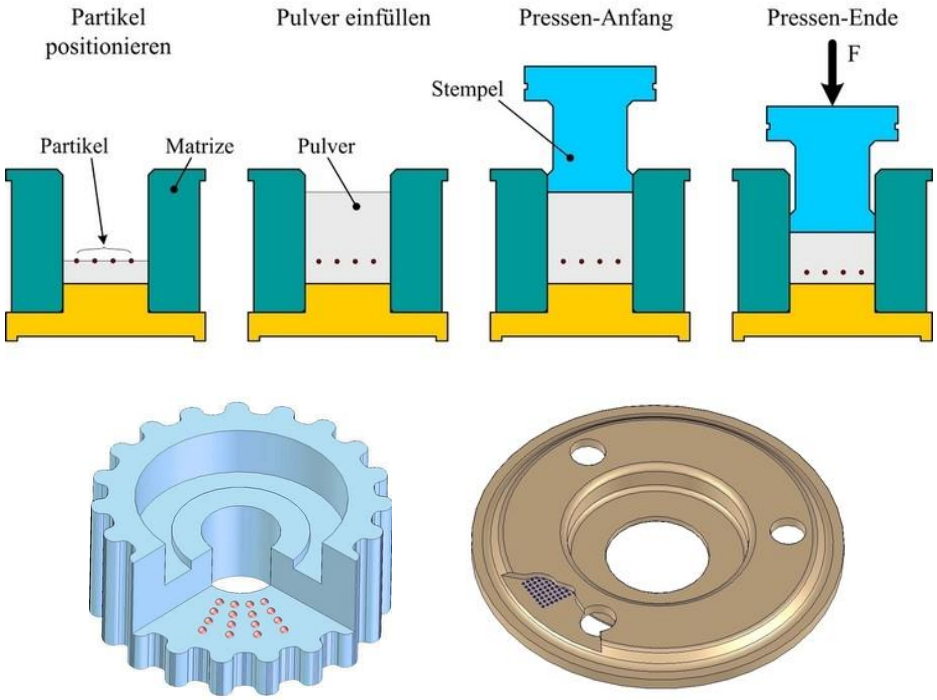


Abbildung A-58: Herstellung einer Markierung innerhalb eines Sinterbauteils (oben) und Beispiele für markierte Bauteile, [Beh-13b] und [Ins-13, Beh-13b]

A.6.3 Nanopartikel

Die Beimischung von Partikeln in der Größe weniger Nanometer in Grundsubstrate ist mit Elektronenmikroskopen nachweisbar.

Quellen: Sok-06, Wel-07

Anhang B Seitens GS1 definierte Codes

In Tabelle B-1 wird deutlich, dass alle Codes durch das durch GS1 weltweit je Unternehmen einmal vergebene Company Prefix eingeleitet und entweder per Definition serialisiert (z. B. SSCC, SGTIN) oder durch einen Application Identifier (siehe [GS1-13c]) individualisierbar sind (z. B. GTIN, GLN, GRAI). Davon ausgenommen sind die GID, RCN, DOD und ADI, die diesem Aufbau nicht folgen, weil diese für spezielle Zwecke mit spezifischen Vorgaben entwickelt wurden.

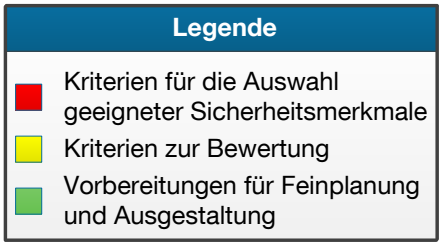
Tabelle B-1: Übersicht über durch GS1 definierte Codes

Kürzel	Bezeichnung	Zusammensetzung	Vornehmlich		Applica-tion Iden-tifier (AI)	Quellen
			Bar-codes	RFID		
GTIN	Global Trade Item Number	Company Prefix + Item Reference + Check Digit	x		x	[GS1-13c] S. 27, S. 140, S. 471
GLN	Global Location Number	Company Prefix + Location Reference + Check Digit	x		x	[GS1-13c] S. 471
SSCC	Serial Shipping Container Code	Extension Digit + Company Prefix + Serial Reference + Check Digit	x	x	x	[GS1-13b] S. 30, [GS1-13c] S. 139
GRAI	Global Returnable Asset Identifier	Company Prefix + Asset Type + Check Digit	x	x	x	[GS1-13b] S. 32, [GS1-13c] S. 82
GIAI	Global Individual Asset Identifier	Company Prefix + Individual Asset Reference	x	x	x	[GS1-13c] S. 24, S. 83, S. 471
GSRN	Global Service Relation Number	Company Prefix + Service Reference + Check Digit	x	x	x	[GS1-13b] S. 33, [GS1-13c] S. 471
GDTI	Global Document Type Identifier	Company Prefix + Document Type + Check Digit	x	x	x	[GS1-13b] S. 33, [GS1-13c] S. 471
GSIN	Global Shipment Identification Number	Company Prefix + Shipper Reference + Check Digit	x		x	[GS1-13c] S. 471
GINC	Global Identification Number for Consignment	Company Prefix + Freight Forwarder's or Carrier's transport reference	x		x	[GS1-13c] S. 471
GCN	Global Coupon Number	Company Prefix + Coupon Reference	x		x	[GS1-13c] S. 125, S. 471
SGTIN	Serialized Global Trade Item Number	GTIN + Serial Number		x		[GS1-13b] S. 29
SGLN	Global Location Number With or Without Extension	GLN + Extension component (AI 414)	x	x		[GS1-13b] S. 31
CPI	Component / Part Identifier	Company Prefix + Component/Part Reference + Serial Number		x		[GS1-13b] S. 37
GID	General Identifier	General Manager Number + Object Class + Serial Number		x		[GS1-13b] S. 34
RCN	Restricted Circulation Number	Prefix + Item Reference + Check Digit	x			[GS1-13c] S. 64 ff.
DOD	US Department of Defense Identifier	defined by United States Department of Defense		x		[GS1-13b] S. 35
ADI	Aerospace and Defense Identifier	defined in the Air Transport Association Spec 1041 2000 and the US Department of Defense Guide to Uniquely 1042 Identifying items		x		[GS1-13b] S. 35

Anhang C Definition aller technischen Auswahlkriterien

Die Beschreibung der Kriterien aus Abbildung 7-3, S. 108 ist teilweise angelehnt an die Vorveröffentlichung des Autors in *Günthner* „Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung. Bestimmung schützenswerter Bauteile, Auswahl von Kennzeichnungstechnologien und Gestaltung des Schutzsystems“ [Gün-11a].

Die im Folgenden verwendeten farblichen Markierungen sind identisch zu den Inhalten in Abschnitt 7.1.1, S. 108 belegt:



C.1 Authentifizierungsinformation

Die Authentifizierungsinformation ist die Information, die auf dem zur Authentifizierung einer Ware angebrachten Kennzeichen repräsentiert sein soll. Diese Information wird hierfür in eine vom verwendeten Sicherheitsmerkmal abhängigen Symbolik umgewandelt. Mögliche Ausprägungen sind:

- Originalitätskennzeichen mit dem Informationsgehalt „0/1“, also „nicht original“ oder „original“
- Unikatkennzeichen mit dem Informationsgehalt „0/1“ und Aussagen über die Identität der individuellen Ware

Auswirkungen auf die Technologieauswahl:
Die gewünschte Authentifizierungsinformation schränkt die Menge der nutzbaren Sicherheitsmerkmale ein. Wenn beispielsweise alle Originalwaren anhand Unikatkennzeichen individuell unterscheidbar sein sollen, fallen alle reinen Originalitätskennzeichen aus der Menge der passenden Merkmale heraus.

C.2 Weitere Daten

Weitere Daten sind Daten, die im Sicherheitsmerkmal selbst als Zusatzinformationen zur Verfügung stehen sollen, die jedoch über die Bestimmung der Originalität hinausgehen. Mögliche Ausprägungen der weiteren Daten sind Nummern oder alphanumerische Zeichen.

Auswirkungen auf die Technologieauswahl:
Wenn weitere Daten im Sicherheitsmerkmal repräsentiert sein sollen, schränkt dies die Menge der nutzbaren Kennzeichen aufgrund der hierfür notwendigen Technologieeigenschaften des Kennzeichens ein. In diesem Fall können reine Originalitätskennzeichen nicht verwendet werden.

C.3 Variable Daten

Variable Daten sind Daten, die im Sicherheitsmerkmal des Produkts gespeichert und während der Lebensdauer des Produkts verändert oder ergänzt werden sollen.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium ist zur Bewertung wichtig, d. h. nach der Auswahl passender Kennzeichen mittels der „Kriterien für die Auswahl geeigneter Sicherheitsmerkmale“ ( ) werden die verbleibenden Technologien mit Hilfe dieses Kriteriums hinsichtlich ihrer Funktionalität, variable Daten zu halten, bewertet.

C.4 Branding

Branding bezeichnet die Markierung eines Produkts mit einem eingetragenen Markenzeichen, welches das Markenbewusstsein nutzt oder steigert.

Auswirkungen auf die Technologieauswahl:
Diese Forderung wird bei der Feinplanung und Ausgestaltung des gewählten Sicherheitsmerkmals berücksichtigt. Bei einigen Sicherheitsmerkmalen ist es möglich, beispielsweise ein Markenzeichen mit zu integrieren. Damit erhält man einen doppelten Schutz: Den Schutz durch das kopiersichere Kennzeichen und den juristischen Schutz aus dem angemeldeten Markenzeichen (siehe Kapitel 6, S. 101).

C.5 Ort des Sicherheitsmerkmals

Dieses Kriterium fasst drei Unterkriterien zusammen:

- ↳ Produkt oder Verpackung
  - Produkt
  - Verpackung
- ↳ Untergrund
- ↳ Bauraum

Während das erste zu den Kriterien zur Auswahl geeigneter Sicherheitsmerkmale zählt, gehören die beiden weiteren zu den Kriterien für die Feinplanung und Ausgestaltung.

C.5.1 Produkt oder Verpackung

Das Kennzeichen kann entweder auf der Verpackung oder auf dem Produkt selbst angebracht sein – je nachdem, ob das Produkt nach dem Auspacken noch gekennzeichnet sein muss. Da es das Ziel ist, Bauteile während der gesamten Lebensdauer als Originale zu erkennen, ist ein Kennzeichnen der Verpackung zweitrangig.

Auswirkungen auf die Technologieauswahl:
Technologien, die nur für Verpackungen entwickelt wurden, sind zur Kennzeichnung der Produkte selbst nicht nutzbar und umgekehrt.

C.5.2 Untergrund

Bei Anbringung des Sicherheitsmerkmals am Produkt selbst steht oftmals lediglich ein bestimmter Untergrund zur Verfügung.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium wird nur bei der Feinplanung und Ausgestaltung des Sicherheitsmerkmals benutzt. Bezüglich des Untergrunds kann festgestellt werden, dass dies selten zu echten Einschränkungen in der Auswahl der Technologien führt, denn die Sicherheitsmerkmale selbst können normalerweise entsprechend angepasst werden.

C.5.3 Bauraum

Bei Anbringung des Sicherheitsmerkmals am Produkt selbst ist der Bauraum oftmals räumlich begrenzt.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium wird nur bei der Feinplanung und Ausgestaltung des Sicherheitsmerkmals benutzt. Bezüglich des zur Verfügung stehenden Platzes zur Anbringung eines Sicherheitsmerkmals kann festgestellt werden, dass dies selten zu echten Einschränkungen in der Auswahl der Technologien führt, denn die Sicherheitsmerkmale selbst können normalerweise in Form und Größe angepasst werden.

C.6 Verbindung zwischen Sicherheitsmerkmal und Produkt

Ein Sicherheitsmerkmal kann auf verschiedene Arten am Produkt angebracht werden. Dabei stehen folgende zur Auswahl:

- Einbringen in das Produkt
- Nutzung einer vorhandenen Oberfläche(nstruktur)
- Erzeugung einer besonderen Oberfläche mittels Oberflächenänderung
- Oberflächenauftrag
- Etikett

Ein Auf- / Einbringen eines Sicherheitsmerkmals auf / in ein Etikett ist selbstverständlich immer möglich, bei expliziter Nennung allerdings ist nur diese Möglichkeit realisierbar.

Auswirkungen auf die Technologieauswahl:
Die Sicherheitsmerkmale unterscheiden sich hinsichtlich ihrer Möglichkeiten zur Auf- / An- / Einbringung auf / an / in ein Produkt. Dieses Kriterium ist allerdings lediglich nach Auswahl passender Kennzeichen mittels der „Kriterien für die Auswahl geeigneter Sicherheitsmerkmale“ ( ) wichtig und es werden die verbleibenden Technologien mit Hilfe dieses Kriteriums hinsichtlich ihrer Möglichkeit bzgl. der Verbindung zwischen Sicherheitsmerkmal und Produkt bewertet.

C.7 Belastungen am Einbauort

Die Belastungen auf das Sicherheitsmerkmal am Einbauort im Betrieb der jeweiligen Maschine oder Anlage werden durch die Umgebungsbedingungen beschrieben. Entscheidende Belastungen sind:

- Abrasive Prozesse (Scheuern, Kratzen)
- Verschmutzung, Beschichtung, Lackierung
- Beschleunigung, Schwingung
- lipophile Stoffe (Öle, Kühlschmiermittel)
- Säuren, Basen, Lösungsmittel
- Luftfeuchtigkeit
- hohe / tiefe Temperatur
- Druck
- magnetische / elektrische Energiedichten

Auswirkungen auf die Technologieauswahl:
Die Umgebungsbedingungen am Einbauort sind deshalb wichtig, weil das Bauteil auch nach dem Einbau authentifizierbar sein soll. Jedoch können mit entsprechendem Know-how die Sicherheitsmerkmale meist so ausgestaltet werden, dass diese den Belastungen am Einbauort standhalten. Daher wurde dieses Kriterium für die Feinplanung und Ausgestaltung eingeordnet.

C.8 Authentifizierungshäufigkeit

Die Authentifizierungshäufigkeit benennt die Anzahl, wie oft ein Produkt authentifiziert werden muss. Als Klassifizierung genügen die Ausprägungen

- einmal,
- mehrmals,
- unbegrenzt.

Auswirkungen auf die Technologieauswahl:
Unterschiedliche Kennzeichen ermöglichen die Prüfung der Echtheit technologieabhängig entweder einmal, mehrere Male oder unbegrenzt oft. Der Vergleich der benötigten mit der möglichen Authentifizierungshäufigkeit der einzelnen Technologien führt zum Ausschluss von Sicherheitsmerkmalen.

C.9 Zugänglichkeit bei der Prüfung

Zur Authentifizierung eines Produkts am Einsatzort sind abhängig vom verwendeten Sicherheitsmerkmal unterschiedliche Zugänglichkeiten notwendig. Meist wird berührungslos, also optisch oder (elektro-)magnetisch geprüft. Es gibt aber auch Prüfvorgänge, die nur nach einer Berührung eine Authentifizierung ermöglichen. Es gibt somit für dieses Kriterium zwei Ausprägungen:

- berührend
- berührungslos

Auswirkungen auf die Technologieauswahl:
Sollte ein Bauteil im verbauten Zustand nur berührungslos geprüft werden können, fallen alle Sicherheitsmerkmale weg, die für eine erfolgreiche Authentifizierung eine Berührung voraussetzen. Bei berührungslosen Verfahren kann auch noch zwischen optischen, die eine Sichtverbindung voraussetzen, und (elektro-)magnetischen Verfahren unterschieden werden.

C.10 Infrastruktur für Prüfung

Die Infrastruktur für den Prüfvorgang wird durch die vorhandenen Medien am Ort der Prüfung bestimmt. Dabei reicht die Unterscheidung zwischen:

- Keine
- Strom
- Datenverbindung

Auswirkungen auf die Technologieauswahl:
Je nach gewünschtem Prüfaufwand (siehe Anhang C.11) und gewünschtem Automatisierungsgrad (siehe Anhang C.12) ist die Verwendung bestimmter Verfahren erforderlich, die wiederum unterschiedliche Hilfsmittel und Medien nutzen. Stehen bestimmte Medien für eine Prüfung nicht zur Verfügung, schließt dies Technologien aus.

C.11 Prüfaufwand

Der Prüfaufwand umfasst den akzeptablen Aufwand zur Feststellung der Originalität. Dabei sind zwei Aspekte zu betrachten:

- ↳ für die Prüfung notwendige Hilfsmittel
  - keine Hilfsmittel
  - portable Hilfsmittel
  - festinstallierte Hilfsmittel
  - Labortechnik
- ↳ für die Prüfung notwendige Zeitdauer

Während das erste Kriterium zum Ausschluss von Technologien führen kann, wird das zweite Kriterium bei der Feinplanung und Ausgestaltung herangezogen.

C.11.1 Für die Prüfung notwendige Hilfsmittel

Die notwendigen Hilfsmittel können in vier Kategorien unterschieden werden. „Keine“ bedeutet, dass ein geschulter Prüfer die Authentifizierung manuell durchführen kann. Unter „portable Hilfsmittel“ werden alle Mittel zur Authentifizierung verstanden, welche ein Mitarbeiter ortsunabhängig zur Authentifizierung einsetzen kann. „Festinstallierte Hilfsmittel“ hingegen sind Geräte, die in Maschinen und Anlagen eingebaut und somit fest installiert werden können. Dies umfasst einerseits Geräte, die eine vollautomatische Authentifizierung eingebauter Bauteile ermöglichen, andererseits aber auch Geräte, welche von einem Maschinenbediener geführt zur Anwendung gebracht werden, z. B. ein an einer Maschine fest angeschlossener Handscanner. Unter „Labortechnik“ sind alle Prüfmittel zu verstehen, die nur in einem Labor zur Authentifizierung eines Bauteils verwendet werden.

Auswirkungen auf die Technologieauswahl:
Der Prüfaufwand grenzt je nach gewählter Ausprägung die Menge möglicher Sicherheitsmerkmale stark ein. Ausprägungen wie "keine Hilfsmittel" oder "festinstallierte Hilfsmittel" sind komplementär und haben einen großen Einfluss auf die verbleibende Anzahl möglicher Sicherheitsmerkmale.

C.11.2 Für die Prüfung notwendige Zeitdauer

Die notwendige Zeitdauer ist direkt abhängig vom vorherigen Punkt „Hilfsmittel“. Die Auswahl einer entsprechenden Ausprägung impliziert die zur Verfügung stehende Zeit.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium wird bei der Feinplanung und Ausgestaltung berücksichtigt. Der

zeitliche Faktor ist häufig mit der Festlegung des Hilfsmittels vorfestgelegt, kann aber in gewissen Grenzen noch beeinflusst werden.

C.12 Automatisierungsgrad der Prüfung

Der Automatisierungsgrad gibt an, wie der Prüf- und Authentifizierungsvorgang erfolgen soll. Mögliche Ausprägungen sind:

- manuell
- halbautomatisch
- automatisch
- labortechnisch

„Manuell“ bedeutet, dass ein Prüfer ein Sicherheitsmerkmal eigenhändig oder mit einfachsten Hilfsmitteln (z. B. Testtinten, siehe Anhang A.5.4.11) authentifizieren kann und der Prüfer somit sofort das Ergebnis der Überprüfung erhält. Unter „halbautomatisch“ wird hier eine Prüfung verstanden, bei der technische Hilfsmittel für eine Authentifizierung verwendet werden und das Prüfergebnis in irgendeiner Form elektronisch zur Verfügung steht, z. B. Authentifizierung eines Bauteils mit Hilfe eines an der Maschine festinstallierten Handscanners. Bei einer Prüfung, die „automatisch“ erfolgt, werden Bauteile mit Hilfe eines Prüfgeräts in einer Maschine oder Anlage vollautomatisch erfasst und authentifiziert. Das Prüfergebnis steht der Maschine oder Anlage danach in elektronischer Form zur Verfügung. Bei einer „labortechnisch“ basierten Prüfung müssen die zu prüfenden Produkte zur Authentifizierung in ein Labor gegeben werden. Eine labortechnische Prüfung von Sicherheitsmerkmalen ist selbstverständlich immer durchführbar, bei expliziter Nennung allerdings ist nur diese Möglichkeit realisierbar.

Auswirkungen auf die Technologieauswahl:
Reaktionsmöglichkeiten des Gesamtsystems können bei einer automatischen Prüfung sehr effektiv sein, da ein Vergessen / Umgehen / Manipulieren der Prüfung verhindert wird. Da sich nicht alle Kennzeichnungstechniken zur Automatisierung eignen, fallen bei dieser Ausprägung nicht nutzbare Technologien weg.

C.13 Distanz bei der Prüfung

Die Distanz bei der Prüfung beschreibt den minimal möglichen Abstand zwischen Prüfinstanz (Gerät oder Mensch) und dem Sicherheitsmerkmal während des Prüfvorgangs.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium ist sehr nachrangig, da bereits bei der „Zugänglichkeit bei der Prüfung“ (siehe Anhang C.9) der wesentliche Punkt geklärt wurde. Die Distanz, sofern die Prüfung „nicht berührend“ stattfinden soll, kann bei der Feinplanung und Ausgestaltung des Sicherheitsmerkmals berücksichtigt werden.

C.14 Backup-Prüfung

Die Backup-Prüfung ist ein zweiter Weg der Authentifizierung für den Fall, dass das Haupt-Sicherheitsmerkmal ausfällt. Somit kann das Produkt weiterhin als Original authentifiziert werden.

Auswirkungen auf die Technologieauswahl:
Für die Technologieauswahl ist dieses Kriterium nicht relevant – bei Wunsch nach einer Backup-Prüfung kann das gesamte methodische Vorgehen zur Auswahl eines passenden Sicherheitsmerkmals einfach erneut durchlaufen werden.

C.15 Sicherheit

Die Sicherheit für den Nachweis der Originalität einer Ware kann in drei Bereiche eingeteilt werden:

- Kopiersicherheit
  - einfache Hilfsmittel
  - besondere Ausrüstung
  - quasi nicht fälschbar
- Manipulationssicherheit
- Belastbarkeit der Authentifizierung

Das erste der drei Kriterien gehört zu den „Kriterien zur Bewertung“, die beiden letzten werden bei der Feinplanung und Ausgestaltung des Sicherheitsmerkmals berücksichtigt.

C.15.1 Kopiersicherheit

Die Kopiersicherheit ist eine Grundvoraussetzung dafür, dass ein Kennzeichen als Sicherheitsmerkmal eingestuft wird und ist somit immer gegeben. Jedoch gibt es bei den Sicherheitsmerkmalen Qualitätsunterschiede dahingehend, wie aufwändig ein Nachahmen wirklich ist bzw. eingeschätzt wird. Dafür werden hier die Kategorien

- einfache Hilfsmittel,
- besondere Ausrüstung und
- quasi nicht fälschbar

eingeführt. Die Kategorie „unfälschbar“ wird absichtlich nicht verwendet, weil ein Fälschen theoretisch immer möglich ist.

Auswirkungen auf die Technologieauswahl:
Nach der Auswahl der prinzipiell geeigneten Sicherheitsmerkmale werden diese mit den Kriterien zur Bewertung eingestuft. Dabei wird bei gleicher Eignung verschiedener Technologien das „sicherere“ Kennzeichen gewählt.

C.15.2 Manipulationssicherheit

Die Manipulationssicherheit entsteht durch die konkrete Ausgestaltung der Verbindung zwischen Kennzeichen und Produkt. Diese Verbindung kann durch entsprechende Maßnahmen manipulationssicher gegen z. B. eine Übertragung auf eine andere Ware gestaltet werden.

Auswirkungen auf die Technologieauswahl:
Die Manipulationssicherheit ist vom konkreten Anwendungsfall abhängig und kann in der Feinplanung und Ausgestaltung mit Unterstützung durch Fachexperten erreicht werden.

C.15.3 Belastbarkeit der Authentifizierung

Die Belastbarkeit der Authentifizierung ist abhängig von der Ausgestaltung der Prozesse bei der Herstellung und Markierung der Originalwaren. Durch passende Maß-

nahmen im Prozess muss nachweisbar sichergestellt sein dass jedes Originalprodukt, welches verkauft wird, ein Sicherheitsmerkmal trägt. Zudem dürfen keine Blanko-Sicherheitsmerkmale das Unternehmen verlassen können. Gemeinsam mit passenden Sicherheitsmerkmalen, die in den Kriterien „Manipulationssicherheit“ und „Kopiersicherheit“ sehr stark sind, können Systeme generiert werden, die gerichtsverwertbar sind.

Auswirkungen auf die Technologieauswahl:
Dieses Kriterium wird bei der Ausgestaltung und Feinplanung des Systems berücksichtigt, da hierdurch insbesondere der innerbetriebliche Prozess der Kennzeichnung betroffen ist.

Anhang D Sicherheitsmerkmale mit ihren Eigenschaften

Die in Abschnitt 7.1.1, S. 108 dargestellte Schlüssel-Schloss-Beziehung dient der Bestimmung möglicher Sicherheitsmerkmale aufgrund gegebener technischer Rahmenbedingungen. Um die Voraussetzungen dafür zu schaffen, wurden die technischen Eigenschaften der Sicherheitsmerkmale recherchiert und in der folgenden Gesamttabelle zusammengefasst. Diese Eigenschaften wurden in Kooperation mit den Experten der Schreiner Group GmbH & Co. KG erarbeitet [Sch-10c, Sto-10, Völ-10], entstammen aus den Literaturquellen oder wurden logisch ergänzt.

Das Ergebnis ist die folgende Tabelle, die alle Sicherheitsmerkmale aus Anhang A und alle Eigenschaften entsprechend der technischen Auswahlkriterien aus Abbildung 7-3, S. 108 erfasst, welche der Auswahl geeigneter Sicherheitsmerkmale (■) bzw. der Bewertung (■) dienen. Die Auswahlkriterien, die nur den Vorbereitungen für die Feinplanung und Ausgestaltung dienen, sind in dieser Tabelle nicht abgebildet.

Trotz größter Sorgfalt könnten in dieser Gesamttabelle Irrtümer enthalten sein. Zudem werden die Technologien permanent weiterentwickelt, so dass es sich um den zum Recherchezeitpunkt aktuellen Stand handelt, der sich mit der Zeit verändern wird.

Tabelle D-1: Sicherheitsmerkmale mit ihren Eigenschaften (ohne Gewähr)

Sicherheitsmerkmale				Technische …		
				Daten		
				Authenti-fizierungs-information	Weitere Daten	Variable Daten
				Originalität [1]	ja [3]	ja [4]
				Unikat [2]	nein	nein
Klasse	Gruppe	Kennz. / Technolog. / System	Abschnitt			
Biologisch	-	Antikörper	A.1.1	Originalität	nein	nein
		Desoxyribonukleinsäure (DNA)	A.1.2	-	-	-
		DNA-Sequenz	A.1.2.1	Originalität	nein	nein
		DNA-Strang	A.1.2.2	Originalität	nein	nein
Chemisch	-	Nanotech Barcode	A.2.1	Originalität	nein	nein
Elektrisch / magnetisch / elektromagnetisch	-	Akustomagnetisches Etikett	A.3.1	Originalität	nein	nein
		Elektromagnetisch detektierbare Farbe	A.3.2	Originalität	nein	nein
		Elektromagnetisches Etikett	A.3.3	Originalität	nein	nein
		Elektromagnetische Glasfasern	A.3.4	Originalität	nein	nein
		Mikrochip mit Kontakt	A.3.5	Unikat	ja	ja
		Radiofrequenzidentifikation (RFID)	A.3.6	Unikat	ja	ja
Haptisch	Druckverfahren	Hochdruck	A.4.1.1	Originalität	nein	nein
		Matrixdruck / Nadeldruck	A.4.1.2	Unikat	ja	nein
		Tiefdruck	A.4.1.3	-	-	-
		Intagliodruck / Stichtiefdruck	A.4.1.3.1	Originalität	nein	nein
		Orlof-Technik / Schablonen-einfärbetechnik	A.4.1.3.2	Originalität	nein	nein
		Rastertiefdruck	A.4.1.3.3	Originalität	nein	nein
		Siebdruck	A.4.1.4	Originalität	nein	nein
	Prägen	Blindprägung	A.4.2.1	Originalität	nein	nein
		Heißfolienprägung	A.4.2.2	Originalität	nein	nein
Optisch	Optische Effekte	Durchsichtsfenster	A.5.1.1	-	-	-
		Foliendurchsichtsfenster	A.5.1.1.1	Originalität	nein	nein
		Moiré Magnifier-Element	A.5.1.1.2	Originalität	nein	nein
		Durchsichtsregister	A.5.1.2	Originalität	nein	nein
		Hologramme	A.5.1.3	Originalität	nein	nein
		Laserkippbild	A.5.1.4	Unikat	ja	nein
		Parallaxe	A.5.1.5	Originalität	nein	nein
		Retroreflektierende Folie	A.5.1.6	Originalität	nein	nein
		Wasserzeichen	A.5.1.7	Originalität	nein	nein
	Pre-Press-Druckmerkmale	Anti-Kopier-Muster	A.5.2.1	beides [25]	ja [26]	nein
		Besondere Schriftart	A.5.2.2	Originalität	nein	nein
		Digitale Wasserzeichen	A.5.2.3	Originalität	nein	nein
		Mikrotext	A.5.2.4	Originalität	nein	nein
		Rasterbild	A.5.2.5	Originalität	nein	nein
		Scrambled image / codiertes Bild	A.5.2.6	Originalität	nein	nein
	Spezialdruck	Guillochen	A.5.3.1	Originalität	nein	nein
		Irisdruck / Regenbogendruck	A.5.3.2	Originalität	nein	nein
⋮	⋮	⋮	⋮	⋮		

...	Technische Einflussgrößen (Ausschluss- und Bewertungsgrößen)							
...	Anbringung		Prüfung des Kennzeichens					Sicherheit
...	Ort des Sicherheits-merkmals	Verbindung Merkmal - Produkt	Authenti-fizierungs-häufigkeit	Zugänglich-keit bei der Prüfung	Infra-struktur für Prüfung	Prüfaufwand (Hilfsmittel)	Automa-tisierungs-grad [17]	Kopier-sicherheit
...	Produkt	EI [5]	einmal	berührend	keine [11]	keine	manuell [18]	einfache H. [22]
	Verpackung	OÄ [6]	mehrmals	ber.los [10]	Strom [12]	portabel [14]	halbaut. [19]	besondere A. [23]
		OS [7]	unbegrenzt		Datenverb. [13]	festinstalliert [15]	automatisch [20]	q. n. f. [24]
		OA [8]				Labortechnik [16]	labortech. [21]	
		ET [9]						
	beides	OA / ET	einmal	berührend	keine	portabel	manuell	q. n. f.
	-	-	-	-	-	-	-	-
	beides	OA / ET	mehrmals	berührend	Strom	Labortechnik	labort.	q. n. f.
	beides	OA / ET	mehrmals	berührend	keine	portabel	manuell	q. n. f.
	beides	EI / ET	unbegrenzt	ber.los	(Strom)	portabel / festinstalliert	halbaut.	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	Strom	festinstalliert	halbaut. / automatisch	besondere A.
	beides	OA / ET	unbegrenzt	berührend	Strom	portabel	halbaut.	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	Strom	festinstalliert	halbaut. / automatisch	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut.	besondere A.
	beides	EI	unbegrenzt	berührend	Datenverb.	festinstallliert	halbaut.	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
	beides	OA /ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	Verpackung	ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	-	-	-	-	-	-	-	-
	beides	OA / ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	beides	OÄ	unbegrenzt	berührend	keine	keine	manuell	besondere A.
...	beides	OÄ	unbegrenzt	berührend	keine	keine	manuell	besondere A.
	beides	ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	-	-	-	-	-	-	-	-
	Verpackung	EI	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	Verpackung	ET	unbegrenzt	ber.los	keine	keine	manuell	q. n. f.
	Verpackung	EI	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel	manuell / halbaut.	besondere A. / q. n. f.
	beides	ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine	keine	manuell	q. n. f.
	beides	ET	unbegrenzt	ber.los	Strom	festinstalliert	manuell	besondere A.
	Verpackung	EI [28]	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET [29]	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut. / automatisch	besondere A.
	beides	ET	unbegrenzt	ber.los	keine / Strom	keine / portabel / festinstalliert	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine	portabel	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine	keine / portabel	manuell	besondere A.
	⋮		⋮					⋮

⋮	⋮	⋮	⋮	⋮		
Optisch	**Spezialfarben / Spezialpartikel**	Clustermerkmal	A.5.4.1	Originalität	nein	nein
		Fotochrome Farbe	A.5.4.2	-	-	-
		Reversible fotochrome Farbe	A.5.4.2.1	Originalität	nein	nein
		Irreversible fotochrome Farbe	A.5.4.2.2	Originalität	nein	nein
		Fluoreszenz	A.5.4.3	-	-	-
		Infrarot-Farbe (IR)	A.5.4.3.1	Originalität	nein	nein
		Röntgenlumineszenz	A.5.4.3.2	Originalität	nein	nein
		Tagesleuchtfarbe / Neonfarbe als Echtfarbelement	A.5.4.3.3	Originalität	nein	nein
		Ultraviolette Farbe (UV)	A.5.4.3.4	Originalität	nein	nein
		Interferenz- und Effektfarbe	A.5.4.4	Originalität	nein	nein
		Kippfarbe / optisch variable	A.5.4.5	Originalität	nein	nein
		Magnetisierbare Farbe	A.5.4.6	Originalität	nein	nein
		Metallreagenzfarbe	A.5.4.7	Originalität	nein	nein
		Metamere Farbe	A.5.4.8	Originalität	nein	nein
		Mikrofarbcode	A.5.4.9	Originalität	nein	nein
		Mikropunkte	A.5.4.10	Originalität	ja [27]	nein
		Pen-Reactive-Ink / Reagenzfarbe	A.5.4.11	Originalität	nein	nein
		Phosphoreszenz	A.5.4.12	Originalität	nein	nein
		Sicherheitsfärbemittel	A.5.4.13	Originalität	nein	nein
		Sonderfarbe	A.5.4.14	Originalität	nein	nein
		Spektralsensible Farbe	A.5.4.15	Originalität	nein	nein
		thermoreaktive Farbe	A.5.4.16	-	-	-
		Thermische Pigmente	A.5.4.16.1	Originalität	nein	nein
		Thermochrome Pigmente	A.5.4.16.2	Originalität	nein	nein
	Sonstige	Feuchtstempelabdruck	A.5.5.1	Originalität	nein	nein
		Lasergravur	A.5.5.2	Unikat	ja	nein
		Oberflächenauthentifizierung	A.5.5.3	-	-	-
		Musteroberfläche	A.5.5.3.1	Unikat	nein	nein
		Sprengprägen	A.5.5.3.2	Originalität	nein	nein
		Stochastische Schwankungen im Fertigungsprozess	A.5.5.3.3	Unikat	nein	nein
		Perforation	A.5.5.4	-	-	-
		Laserperforation	A.5.5.4.1	Unikat	ja	nein
		Nadelperforation	A.5.5.4.2	Unikat	ja	nein
		Rauschmustercodes	A.5.5.5	Unikat	ja	nein
		Sicherheitsanstanzung	A.5.5.6	Originalität	nein	nein
		Sicherheitsfaden	A.5.5.7	Originalität	nein	nein
Sonstige	-	Duftstoffe	A.6.1	Originalität	nein	nein
		Markierung pulvermetallurgisch	A.6.2	Unikat	ja	nein
		Nanopartikel	A.6.3	Originalität	nein	nein

	⋮		⋮					⋮
	beides	ET	unbegrenzt	ber.los	keine / Strom	keine/portabel	manuell / halbaut.	besondere A.
	-	-	-	-	-	-	-	-
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell	besondere A.
	beides	OA /ET	einmal	ber.los	keine / Strom	portabel / festinstalliert	manuell	besondere A.
	-	-	-	-	-	-	-	-
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell / halbaut. / automatisch	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	Strom	festinstalliert	halbaut.	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell / halbaut. / automatisch	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET [29]	unbegrenzt	ber.los	Strom	portabel / festinstalliert	halbaut.	q. n. f.
	beides	OA / ET	einmal	berührend	keine	portabel	manuell	besondere A.
	beides	ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell	besondere A.
	beides	EI / OA / ET	unbegrenzt	ber.los	keine	portabel / festinstalliert	manuell	q. n. f.
	beides	OA / ET	unbegrenzt	ber.los	keine	portabel	manuell	besondere A.
	beides	OA / ET	einmal	berührend	keine	portabel	manuell	besondere A.
...	beides	EI / OA / ET	unbegrenzt	beides	Strom	portabel / festinstalliert	labort.	besondere A.
	Verpackung	ET	einmal	berührend	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	portabel / festinstalliert	manuell	besondere A.
	-	-	-	-	-	-	-	-
	beides	OA / ET	einmal	ber.los	keine / Strom	keine / portabel	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	keine / Strom	keine / portabel	manuell	besondere A.
	beides	OA /ET	unbegrenzt	ber.los	keine	keine	manuell	einfache H.
	beides	OÄ / ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	-	-	-	-	-	-	-	-
	Produkt	OÄ	unbegrenzt	ber.los	Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.
	beides	EI / ET	unbegrenzt	ber.los	Datenverb.	portabel / festinstalliert	halbaut.	q. n. f.
	beides	OS	unbegrenzt	ber.los	Datenverb	portabel / festinstalliert	halbaut. / automatisch	q. n. f.
	-	-	-	-	-	-	-	-
	beides	EI / ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	Verpackung	EI / ET	unbegrenzt	beides	keine	keine	manuell	besondere A.
	beides	OA / ET	unbegrenzt	ber.los	Strom / Datenverb.	portabel / festinstalliert	halbaut. / automatisch	q. n. f.
	beides	EI / ET [30]	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	EI / ET [30]	unbegrenzt	ber.los	keine	keine	manuell	besondere A.
	beides	OA / ET	mehrmals	ber.los	Datenver.	portabel	halbaut.	besondere A.
	Produkt	EI	unbegrenzt	ber.los	Strom	festinstalliert	labort.	besondere A.
	beides	EI / ET	unbegrenzt	ber.los	Datenverb.	festinstalliert	labort.	besondere A.

Tabelle D-2: Legende und Fußnoten zu Tabelle D-1

Legende & Fußnoten	
	Kriterien für die Auswahl geeigneter Sicherheitsmerkmale
	Kriterien zur Bewertung
[1]	Originalitätskennzeichen, also Kennzeichen mit fälschungssicheren Merkmalen - entspricht „original" oder "nicht original"
[2]	Unikatkennzeichen, also Kennzeichen mit fälschungssicheren, einmaligen Merkmalen - entspricht „original" oder "nicht original" und einer Aussage über die Identität des individuellen Produkts
[3]	es sollen weitere Daten auf dem Sicherheitsmerkmal abgelegt werden können
[4]	es sollen variable Daten auf dem Sicherheitsmerkmal abgelegt werden können
[5]	EI: Einbringen in das Produkt
[6]	OÄ: Oberflächenänderung am Produkt
[7]	OS: Nutzung der vorhandenen Oberflächenstruktur am Produkt
[8]	OA: Oberflächenauftrag auf das Produkt
[9]	ET: Verwendung eines Etiketts
[10]	berührungslos
[11]	weder Strom noch andere Medien verfügbar
[12]	außer Strom keine weiteren Medien verfügbar
[13]	Strom und eine Datenverbindung mit Zugriff auf einen Server sind vorhanden
[14]	alle Mittel zur Authentifizierung, welche ein Mitarbeiter ortsunabhängig einsetzen kann
[15]	Geräte, die in Maschinen und Anlagen eingebaut und somit fest installiert werden können. Dies umfasst einerseits Geräte, die eine vollautomatische Authentifizierung eingebauter Bauteile umfassen, andererseits aber auch Geräte, welche von einem Maschinenbediener geführt zur Anwendung gebracht werden, z. B. ein an einer Maschine fest angeschlossener Handscanner.
[16]	alle Prüfmittel, die nur in einem Labor zur Authentifizierung eines Bauteils verwendet werden.
[17]	diese Ausprägungen werden entsprechend der „üblichen Verwendung“ angegeben, Weiterentwicklungen der Technologien sind selbstverständlich immer denkbar
[18]	d.h. ein Prüfer kann ein Sicherheitsmerkmal eigenhändig oder mit einfachsten Hilfsmitteln (z. B. Testtinten) authentifizieren und erhält sofort das Ergebnis der Prüfung
[19]	halbautomatisch, d.h. bei einer Prüfung werden technische Hilfsmittel für eine Authentifizierung verwendet und das Prüfergebnis steht in irgendeiner Form elektronisch zur Verfügung, z. B. Authentifzierung eines Bauteils mit Hilfe eines an der Maschine festinstallierten Handscanners.
[20]	d.h. bei einer Prüfung werden Bauteile mit Hilfe eines Prüfgeräts in einer Maschine oder Anlage vollautomatisch erfasst und authentifiziert. Das Prüfergebnis steht der Maschine oder Anlage danach in elektronischer Form zur Verfügung.
[21]	labortechnisch, d.h. für diese Prüfung müssen die zu prüfenden Produkte zur Authentifizierung in ein Labor gegeben werden. Eine labortechnische Prüfung von Sicherheitsmerkmalen ist selbstverständlich immer durchführbar, bei expliziter Nennung allerdings ist nur diese Möglichkeit realisierbar.
[22]	einfache Hilfsmittel
[23]	besondere Ausrüstung
[24]	quasi nicht fälschbar
[25]	abhängig von der Ausführung
[26]	nur, falls bei der Authentifizierungsinformation die Ausprägung "Unikatkennzeichen" gewählt wurde.
[27]	die einzelnen Punkte können auch eine Sachnummer oder einen anderen Code tragen - diese Information ist aber für alle Bauteile gleich
[28]	nur in Papier / Hängeschildchen
[29]	bei Untergrund Papier
[30]	nur in Papier o.ä.

Anhang E Vorlagen für Unternehmen

Tabelle E-1: Auswahl schützenswerter Bauteile gemäß Vorgehen in Abschnitt 5.2.1, S. 87

	Basiskriterien			Optionale Kriterien				
Schützenswerte Bauteile	Sicherheitsrelevanz	Funktionsrelevanz	Gewinnträger	Teile / Produkte mit Alleinstellungsmerkmal	Hohe F&E-/Know-how-Intensität	Gefahr von Imageschäden	Hohe Absatzzahlen	Hybrides Produkt

Tabelle E-2: Angaben der gewünschten Ausprägungen bzgl. der technischen Auswahlkriterien für ein schützenswertes Bauteil gemäß Vorgehen in Abschnitt 7.1, S. 107

	Schützenswertes Bauteil:	
	Kriterium	**Angabe der gewünschten Ausprägung**
Kriterien für die Auswahl geeigneter Sicherheitsmerkmale	Ort des Sicherheitsmerkmals (Produkt oder Verpackung)	
	Authentifizierungshäufigkeit	
	Authentifizierungsinformation	
	Weitere Daten	
	Zugänglichkeit bei der Prüfung	
	Infrastruktur für Prüfung	
	Prüfaufwand (Hilfsmittel)	
	Automatisierungsgrad der Prüfung	
Kriterien zur Bewertung	Variable Daten	
	Verbindung zwischen Sicherheitsmerkmal und Produkt	
	Sicherheit (Kopiersicherheit)	
Vorbereitungen für Feinplanung und Ausgestaltung	Ort des Sicherheitsmerkmals (Untergrund)	
	Ort des Sicherheitsmerkmals (Bauraum)	
	Belastungen am Einbauort	
	Distanz bei der Prüfung	
	Prüfaufwand (Prüfzeit)	
	Sicherheit (Manipulationssicherheit)	
	Sicherheit (Belastbarkeit der Authentifizierung)	
	Branding	
	Backup-Prüfung	

Tabelle E-3: Bestimmung des Gesamtschadens für ein von Produkt- und Markenpiraterie betroffenes, schützenswertes Bauteil gemäß Vorgehen in Abschnitt 7.2, S. 133

Ist-Zustand										
t		0	1	2	3	4	5	6	7	8
N_G	[Stück/Jahr]									-
N_O	[Stück/Jahr]									-
N_K	[Stück/Jahr]									-
U_G	[Tsd. €]									-
U_O	[Tsd. €]									-
$U_{O,verl}$	[Tsd. €]									-
$G_{O,verl}$	[Tsd. €]									-
$CF_{statisch}$	[Tsd. €]									-
$CF_{Barwert}$	[Tsd. €]									

K_0 (ohne R_0)	[Tsd. €]	
R_0	[Tsd. €]	
$S_{0,gesamt}$	[Tsd. €]	

Tabelle E-4: Entwicklung eines Szenarios innerhalb der methodischen Herleitung der Wirtschaftlichkeit der Einführung eines Sicherheitsmerkmals inklusive Gesamtsystem für ein von Produktpiraterie betroffenes, schützenswertes Bauteil gemäß Vorgehen in Abschnitt 7.2, S. 133

Szenario										
t		0	1	2	3	4	5	6	7	8
N_G	[Stück/Jahr]									-
N_O	[Stück/Jahr]									-
N_K	[Stück/Jahr]									-
q_{max}	[%]									-
η_S	[%]									-
$N_{O,Z}$	[Stück/Jahr]									-
$N_{O,G}$	[Stück/Jahr]									-
N_K	[Stück/Jahr]									-
U_G	[Tsd. €]									-
U_O	[Tsd. €]									-
$U_{O,Z}$	[Tsd. €]									-
$U_{O,verl}$	[Tsd. €]									-
I	[Tsd. €]									-
K_{var}	[Tsd. €]									-
$G_{O,verl}$	[Tsd. €]									-
$CF_{statisch}$	[Tsd. €]									-
$CF_{Barwert}$	[Tsd. €]									

K_0 (ohne R_0)	[Tsd. €]	
R_0	[Tsd. €]	
$S_{0,gesamt}$	[Tsd. €]	

Bewertung des Szenarios										
$CF_{Barwert,Diff}$	[Tsd. €]									

K_0 (ohne R_0)	[Tsd. €]	
R_0	[Tsd. €]	
$K_{0,s}$	[Tsd. €]	